Nombre Comercial del Bien o Servicio	SERVICIO DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD
Calidad	El PROVEEDOR debe garantizar que el servicio objeto del presente Anexo Técnico cumpla en su totalidad los requisitos, condiciones y especificaciones aquí establecidos. El PROVEEDOR debe cumplir la Ley 1581 de 2012, el Modelo de Seguridad y Privacidad de la Información - MSPI y las políticas internas de seguridad de la Fiscalía General de la Nación, garantizando la protección, confidencialidad, integridad y disponibilidad de la información durante la ejecución contractual. El servicio debe prestarse aplicando mejores prácticas y marcos de referencia reconocidos, incluyendo, como mínimo: ITIL, ISO 20000, ISO 22301, ISO/IEC 27001, ISO/IEC 27032, COBIT (Control Objectives for Information and Related Technologies), OWASP (Open Web Application Security Project), OSSTMM (Open Source Security Testing Methodology Manual), GDPR (Reglamento General de Protección de Datos), y debe estar alineado con la metodología PMP. Estos marcos de referencia y buenas prácticas tienen carácter referencial y operativo, y su aplicación se verificará mediante los entregables, procedimientos y evidencias que el PROVEEDOR presente durante la ejecución del contrato. El servicio debe ejecutarse conforme a metodologías reconocidas para pruebas de seguridad técnica, tales como NIST SP 800-115 y/o PTES (Penetration Testing Execution Standard). El PROVEEDOR debe contar con las certificaciones ISO/IEC 27001 e ISO 22301, el informe SOC 2 Tipo II y la membresía vigente en FIRST (Forum of Incident Response and Security Teams), con un periodo mínimo de un (1) año desde su obtención, así como cumplir con las normativas aplicables de protección de datos personales, conforme a lo requerido por la ENTIDAD. Estas certificaciones no constituyen requisito habilitante ni deberán presentarse con la oferta. Serán exigibles al inicio del contrato, momento en el cual el PROVEEDOR deberá aportar la evidencia documental que acredite su vigencia, la antigüedad mínima señalada y un alcance que comprenda expresamente los servicios, plataformas, infraestructura, procesos y ubicaciones desde los cuales se atenderá a la ENTIDAD. Las certificaciones y la membresía FIRST podrán ser acreditadas por el PROVEEDOR, por cualquiera de los integrantes de la estructura plural, por su filial, por su aliado autorizado o por el SOC, MSSP o proveedor especializado que efectivamente participe en la prestación del servicio, siempre que se evidencie su relación directa con el alcance del servicio y su disponibilidad durante toda la ejecución contractual. Para los servicios SaaS, cloud o similares operados directamente por el fabricante, podrán ser acreditadas por dicho fabricante u operador del servicio. La certificación ISO/IEC 27001 deberá corresponder a un sistema de gestión de seguridad de la información vigente y con alcance relacionado con los servicios de ciberseguridad. Esta certificación podrá ser aportada por el PROVEEDOR individual o por el integrante del proponente plural que tenga a su cargo la operación principal de los servicios de seguridad. Para los componentes críticos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	de continuidad y recuperación, el responsable de su operación deberá acreditar certificación ISO 22301 vigente. Se deberá aportar un informe SOC 2 Tipo II vigente cuyo alcance comprenda expresamente la plataforma, infraestructura o servicio que será utilizado para atender a la ENTIDAD. El informe deberá ser emitido por una firma de auditoría independiente y competente, con base en los Trust Services Criteria definidos por AICPA, corresponder al último periodo auditado disponible y tener fecha de emisión no superior a doce (12) meses anteriores a la fecha de su acreditación al inicio del contrato. Cuando exista un periodo posterior no cubierto por el informe, deberá aportarse una carta puente o declaración de continuidad de controles suscrita por la organización auditada. Cuando la solución incluya servicios SaaS, cloud o plataformas operadas directamente por un fabricante o tercero, el informe podrá ser aportado por el fabricante u operador del servicio. La antigüedad mínima de un (1) año se contará desde la fecha de emisión del primer informe SOC 2 Tipo II de la organización que lo acredite. No se aceptarán informes SOC 2 Tipo I, informes en trámite ni documentos equivalentes. La carta puente o declaración de continuidad de controles deberá informar si se han presentado cambios materiales en el sistema o servicio, si los controles evaluados continúan operando, si se han identificado incidentes, salvedades o deficiencias relevantes y si existen modificaciones en subservicios, centros de datos, plataformas o procesos cubiertos. El informe SOC 2 Tipo II deberá desarrollarse bajo los estándares profesionales aplicables y su alcance deberá comprender expresamente los servicios, plataformas, infraestructura, centros de operación o centros de datos desde los cuales se prestarán los servicios ofertados y, como mínimo, el criterio de Seguridad y, cuando resulten aplicables al servicio, los criterios de Disponibilidad, Confidencialidad, Integridad del Procesamiento y Privacidad. La ENTIDAD verificará como mínimo la identidad y competencia del auditor independiente, el periodo cubierto por el examen, la descripción y límites del sistema evaluado, los servicios, ubicaciones y organizaciones de subservicio incluidos, los Trust Services Criteria evaluados, la opinión del auditor, las excepciones, observaciones o deficiencias identificadas, los controles complementarios que deban implementar la ENTIDAD o el PROVEEDOR y la correspondencia entre el alcance auditado y la solución ofertada. La presentación del informe no exime al PROVEEDOR de sus obligaciones sobre seguridad, disponibilidad, continuidad, confidencialidad, respuesta a incidentes, cumplimiento de ANS y protección de la información durante la ejecución contractual. Cuando el informe tenga restricciones de distribución o confidencialidad, podrá suministrarse mediante un mecanismo de consulta controlada definido por la ENTIDAD, sin perjuicio de la obligación del PROVEEDOR de aportar la evidencia necesaria para su validación. La membresía vigente en FIRST podrá ser acreditada por el CSIRT del PROVEEDOR, el equipo responsable de la operación o el PSIRT del fabricante, según corresponda al alcance evaluado. Esta membresía será aceptada como evidencia complementaria de capacidad de coordinación y respuesta a incidentes, pero no sustituirá las obligaciones contractuales de atención, contención, investigación, recuperación y cumplimiento de los ANS. El PROVEEDOR debe cumplir durante toda la ejecución con la normativa colombiana aplicable en materia de protección de datos personales, seguridad de la información, confidencialidad, transferencia o transmisión de información, gestión de incidentes, conservación, devolución y eliminación segura de los datos tratados.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Las certificaciones, informes y acreditaciones deberán estar vigentes y su alcance deberá guardar relación directa con las plataformas, procesos, ubicaciones y servicios utilizados para atender a la ENTIDAD. No se aceptarán certificaciones corporativas genéricas cuyo alcance no permita verificar dicha relación. No se aceptarán certificaciones o informes en proceso de obtención, de emisión o en trámite, ni mecanismos o documentos equivalentes. El PROVEEDOR debe presentar al inicio del contrato, en el formato dispuesto por la ENTIDAD, según aplique a cada componente de la solución ofertada, certificación, carta o soporte emitido por el fabricante, partner autorizado, proveedor cloud, marketplace, MSSP, operador autorizado o canal competente, mediante el cual se evidencie su capacidad para suministrar, implementar, administrar, operar y soportar las tecnologías incluidas en la oferta. Podrá presentarse una (1) certificación o carta por fabricante, siempre que identifique expresamente todos los componentes de dicho fabricante incluidos en la oferta y acredite la capacidad para suministrar, implementar, administrar, operar y soportar las tecnologías ofertadas. Las certificaciones del personal deberán corresponder a las tecnologías, plataformas o servicios efectivamente ofertados y utilizados en la prestación del servicio, sin que se exijan certificaciones genéricas sobre fabricantes o componentes no incluidos en la propuesta. En todo caso, el PROVEEDOR mantendrá la responsabilidad integral frente al cumplimiento del objeto contractual, los ANS y las obligaciones técnicas exigidas por la ENTIDAD. La totalidad de las plataformas, equipos y dispositivos que conforman la solución ofertada en el presente Anexo, incluyendo, entre otros, firewalls, appliances, sensores, servidores, equipos de red, agentes y demás componentes de hardware y software, deben cumplir con la Sección 889 de la NDAA (National Defense Authorization Act). Lo anterior deberá acreditarse con al inicio de la ejecución del contrato mediante certificaciones, declaraciones o documentos emitidos por el fabricante o por quien tenga competencia para acreditar dicha condición, sin perjuicio de las verificaciones que la ENTIDAD pueda realizar. **Eficiencia energética y requisitos ambientales de los equipos de seguridad.** El CONTRATISTA deberá garantizar que los equipos físicos que suministre e instale para la prestación de los servicios de seguridad digital y ciberseguridad cumplan la certificación ENERGY STAR® vigente o una certificación ambiental equivalente, como EPEAT, TCO Certified u otra expedida por un organismo reconocido internacionalmente con criterios de eficiencia energética iguales o superiores. Esto incluye firewalls externos e internos, sistemas de detección y prevención de intrusos, plataformas de mitigación de ataques DDoS, servidores, sistemas de almacenamiento y demás dispositivos de la solución. Las fuentes de alimentación de estos equipos deberán contar con certificación 80 PLUS o equivalente. Para los equipos cuya categoría no esté cubierta por las certificaciones mencionadas, el CONTRATISTA deberá acreditar el cumplimiento mediante una declaración del fabricante. Dicha declaración deberá venir acompañada de la ficha técnica en la que consten el consumo de energía en operación y en reposo y las funciones de ahorro de energía disponibles. Cuando los servicios se presten total o parcialmente desde la nube o desde infraestructura del CONTRATISTA o de terceros, este requisito no aplicará a esos componentes. En ese caso, el CONTRATISTA informará las prácticas de eficiencia energética de los centros de datos utilizados, como certificaciones ISO 50001 o ISO 14001 o el indicador de eficiencia energética PUE (Power Usage Effectiveness). El cumplimiento se acreditará con la entrega de los certificados, registros o

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	declaraciones vigentes de cada modelo ofertado, los cuales serán verificados por la supervisión o la interventoría antes de la aceptación de los equipos. Esta exigencia se enmarca en la política de Compra Pública Sostenible y en los lineamientos de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente.
Generalidades	El PROVEEDOR debe prestar un Servicio Gestionado de Seguridad Digital y Ciberseguridad para la Fiscalía General de la Nación, que incluya la administración, operación, monitoreo, análisis, control y mitigación de amenazas, eventos e incidentes, con capacidades de detección, investigación, remediación, gestión de vulnerabilidades y vigilancia digital. Este servicio debe soportarse en una solución tecnológica de última generación que permita colectar, retener, correlacionar y monitorear eventos de seguridad de la infraestructura TI y de las herramientas de seguridad de la ENTIDAD, garantizando su disponibilidad operativa. La prestación será continua 7x24 durante todo el periodo contractual. La herramienta ITSM institucional es el único sistema de registro (SoR - System of Record) para la gestión ITIL del contrato. Todo incidente, requerimiento, problema y cambio asociado a los servicios S1 a S23 debe gestionarse en el ITSM mediante integración técnica con idempotencia y trazabilidad. Esta plataforma no hace parte del presente proceso; por tanto, el PROVEEDOR debe integrarse a la versión vigente y soportar futuras migraciones bajo coordinación con su dueño funcional. Asimismo, el PROVEEDOR debe consumir y enriquecer la CMDB institucional, vinculando cada alerta, incidente, ticket y evidencia al Configuration Item correspondiente, conforme a la práctica SACM (ITIL 4). El PROVEEDOR debe integrar todos los servicios con la Plataforma de Observabilidad institucional, siguiendo los protocolos y conectores definidos por dicha plataforma, la cual constituye el sistema oficial de verificación del cumplimiento de los ANS contractuales. Esta plataforma no se contrata en el presente proceso. La autenticación, autorización y MFA se realizarán mediante el Directorio Activo institucional y el proveedor de identidad definido por la ENTIDAD (Entra ID u otro equivalente). La plataforma SIEM del SOC como servicio (numeral S10) dedicada y exclusiva para la ENTIDAD será la plataforma central de logs de seguridad, con retención WORM de 36 meses. La Plataforma de Observabilidad consumirá únicamente eventos correlacionados y métricas, no logs crudos. El alcance cuantitativo de los servicios se regirá por el Anexo Técnico de Línea Base, que el PROVEEDOR debe asumir como inventario inicial. Las soluciones incluidas en el presente anexo deberán soportar y permitir aplicar políticas de uso de protocolos y algoritmos criptográficos seguros y vigentes, incluyendo mecanismos para restringir o deshabilitar versiones, protocolos o suites criptográficas que sean consideradas obsoletas, vulnerables o no recomendadas por las mejores prácticas de seguridad. Los valores de desempeño ofertados deberán corresponder a escenarios con las funciones de inspección y seguridad habilitadas utilizando configuraciones criptográficas compatibles con los estándares de seguridad exigidos por la ENTIDAD. Esto dentro del plazo de ejecución del contrato.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Toda capacidad de rendimiento ofertada para componentes de inspección en línea deberá corresponder a escenarios de operación con las funcionalidades de seguridad requeridas por la ENTIDAD habilitadas y operando de forma concurrente. El OFERENTE debe declarar expresamente el modo de operación utilizado para la medición, las funcionalidades activas, las condiciones de tráfico, el alcance de la inspección TLS cuando aplique, y los parámetros relevantes para la validación del desempeño. Cuando el componente ejecute inspección o descifrado TLS, el rendimiento declarado deberá corresponder a condiciones representativas de operación con inspección activa del tráfico aplicable, y no únicamente a valores nominales, de laboratorio, de solo detección, monitoreo, SPAN, TAP, flujo pasivo, inspección de certificado o metadatos del handshake. La evidencia podrá acreditarse mediante ficha técnica oficial del fabricante, documentación técnica, informe de laboratorio del fabricante o pruebas de aceptación acordadas con la ENTIDAD, siempre que permita verificar la correspondencia entre el valor ofertado y el escenario documentado. Esta exigencia no implica una metodología propietaria, marca, fabricante o arquitectura específica, sino una condición de comparabilidad, verificabilidad y adecuada supervisión contractual del desempeño ofertado. A discreción del PROVEEDOR, los componentes actualmente disponibles en la ENTIDAD pueden ser utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación de los servicios, siempre que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso. La plataforma de Observabilidad institucional corresponde al sistema oficial de medición y verificación de los ANS y KPIs del contrato. Las soluciones operativas especializadas (monitoreo de conectividad, SIEM/SOAR del SOC, entre otras) deben integrarse obligatoriamente con dicha plataforma, la cual actuará como capa unificada de consolidación, visualización y validación de la información, sin perjuicio de que cada componente mantenga su consola técnica propia para operación. La solución SASE ofertada debe corresponder a una arquitectura nativamente integrada, en la que las capacidades núcleo del servicio —SD-WAN, SWG, CASB, FWaaS, ZTNA y DLP de navegación— operen bajo un único sistema operativo o plataforma, un único plano de control, un lago de datos común y una consola de administración centralizada, evitando integraciones de terceros que generen dependencia operativa o inconsistencias de política en la ruta del tráfico de usuarios. Esta exigencia: (i) aplica exclusivamente al servicio SASE/SSE y no se extiende a los demás servicios del presente anexo, cuyos componentes podrán ser de fabricantes distintos, en un esquema multivendor entre servicios; (ii) no

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	implica exigir un agente único en el dispositivo final ni que capacidades complementarias (aislamiento remoto de navegación, seguridad DNS, monitoreo de experiencia digital) residan en un mismo agente, siempre que se integren de forma nativa a la consola y al lago de datos del servicio. La arquitectura SASE/SSE integrada no implica la exigencia de un agente único obligatorio en el endpoint. No obstante, el PROVEEDOR debe garantizar e informar que los agentes, servicios, extensiones, módulos o componentes residentes que su solución requiera instalar en los dispositivos finales, indicando su función, mecanismo de despliegue, ciclo de actualización, compatibilidad por sistema operativo, consumo estimado de CPU, memoria y almacenamiento, y condiciones de coexistencia con otras herramientas de seguridad. Esta información debe ser verificable durante el piloto, las pruebas de aceptación y el despliegue por fases, garantizando que no se genere degradación material del desempeño del endpoint, conflictos operativos ni afectación de los ANS del servicio; y (iii) no exime al PROVEEDOR de garantizar la integración abierta, interoperable y multivendor de la plataforma SASE con el SOC (SIEM/SOAR), la herramienta ITSM, la plataforma de Observabilidad y los demás servicios del anexo, mediante mecanismos estándar como APIs, Syslog RFC5424, webhooks, conectores estándar y STIX/TAXII o formatos equivalentes cuando aplique, sin que se acepten restricciones que generen dependencia tecnológica injustificada o degradación funcional en entornos multivendor. El PROVEEDOR debe garantizar la disponibilidad total del licenciamiento contratado desde las fases iniciales del servicio. No obstante, la activación de usuarios y endpoints debe realizarse de manera progresiva conforme al plan de migración definido por la ENTIDAD. La interventoría verificará tanto la capacidad instalada como la correcta asignación y uso del licenciamiento durante la ejecución del contrato. Se realizará cobro bajo demanda por uso de las licencias basadas en nube, conforme a los precios unitarios y reglas de activación establecidos. Las referencias a proveedores de nube, suites de colaboración, plataformas de identidad, sistemas operativos, bases de datos y servicios de integración corresponden a tecnologías existentes o previstas en la línea base institucional y se exigen únicamente para efectos de compatibilidad, interoperabilidad, cobertura y administración del entorno de la ENTIDAD. No constituyen una exigencia de marca para los componentes que sean objeto de suministro abierto, salvo en los servicios cuyo objeto sea expresamente la administración de una plataforma existente. **Neutralidad tecnológica y referencias al entorno existente.** Las marcas, fabricantes, productos, modelos, servicios cloud, sistemas operativos, motores de bases de datos, APIs y demás denominaciones tecnológicas identificadas en el presente Anexo Técnico corresponden, según aplique, a componentes actualmente instalados, licenciados, habilitados, utilizados o previstos en la línea base tecnológica de la ENTIDAD. Su mención tiene como finalidad establecer condiciones de administración, transición, compatibilidad, interoperabilidad, integración, soporte y continuidad, y no constituye una exigencia de marca para

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

los componentes nuevos, alternativos o de reemplazo que deba suministrar el PROVEEDOR, salvo en aquellos servicios cuyo objeto sea expresamente la administración de una tecnología existente. Las soluciones alternativas deben acreditar capacidades iguales o superiores y garantizar integración con el entorno institucional, sin restricciones que generen dependencia tecnológica injustificada.
Valoración económica de los servicios S1 a S23. Los servicios S1 a S23 del presente anexo corresponden a capacidades técnicas que integran el Servicio Gestionado de Seguridad Digital y Ciberseguridad. Su valoración económica debe realizarse en los renglones previstos en el Formato de Oferta Económica, principalmente en las pestañas «D2. Seguridad», «P6. Perfiles» y «GG. Gastos Generales, Transición y Administración», según corresponda a licenciamiento, operación, perfiles, integración, transición o componentes transversales. No se crean renglones independientes para cada servicio; los servicios que no se encuentren individualizados en el Formato deben ser incorporados por el OFERENTE dentro de los ítems existentes, sin doble cobro ni reconocimiento económico adicional, manteniéndose la obligación de incluir todos los costos directos e indirectos necesarios para el cumplimiento integral de los anexos técnicos, los ANS, la operación 7x24, las integraciones y los entregables contractuales.

Equivalencia de escalas de severidad y prevalencia de los ANS. La matriz de severidades S1 a S4 utilizada en el presente anexo se corresponde con las prioridades definidas en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio así: S1 (Crítico) equivale a P1; S2 (Alto) equivale a P2; y S3 (Medio) y S4 (Bajo) equivalen a P3. Los tiempos de atención, resolución y escalamiento contractualmente exigibles, su método de medición y las penalidades aplicables son los definidos en el Anexo Técnico 5; los ANS aplicables a los servicios del presente anexo quedan establecidos de forma única en el Anexo Técnico 5. El presente anexo describe las especificaciones técnicas de los servicios y no establece ANS propios; cualquier mención a tiempos, disponibilidad o niveles de servicio contenida en él se rige por lo dispuesto en el Anexo Técnico 5.

Independientemente de que la solución ofertada corresponda a una arquitectura de único fabricante o a una arquitectura multivendor, el PROVEEDOR debe suministrar y mantener vigente, durante toda la ejecución contractual, el licenciamiento, las suscripciones y los servicios de soporte empresarial directo y priorizado con cada fabricante de las soluciones, plataformas y componentes que soporten la operación de los servicios ofertados.
El soporte empresarial deberá contar con cobertura continua 7×24×365, permitir la apertura y escalamiento prioritario de casos directamente ante el fabricante e incluir, como mínimo:

- Acceso a asistencia técnica especializada y a los niveles superiores de escalamiento.
- Diagnóstico y resolución de incidentes críticos.
- Actualizaciones de software y firmware.
- Parches de seguridad, correcciones y nuevas versiones soportadas.
- Acceso a bases de conocimiento y herramientas de diagnóstico.
- Gestión de vulnerabilidades y alertas técnicas del fabricante.
- Garantía, reparación y reemplazo de equipos, módulos, partes o componentes.
- Acompañamiento durante incidentes mayores, ventanas de mantenimiento y procesos de actualización o migración.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	En arquitecturas multivendor, esta obligación se aplicará individualmente a cada fabricante, plataforma y componente que intervenga en la prestación de los servicios. El PROVEEDOR es responsable de coordinar los diferentes soportes y de gestionar integralmente los incidentes hasta su solución definitiva, sin trasladar a la ENTIDAD controversias relacionadas con interoperabilidad, asignación de responsabilidades o escalamiento entre fabricantes. El PROVEEDOR debe garantizar, sin costo adicional para la ENTIDAD, la reparación o sustitución de cualquier equipo, módulo, parte o componente defectuoso, degradado, incompatible o que comprometa la seguridad, capacidad, disponibilidad o continuidad del servicio. El reemplazo deberá efectuarse dentro de los tiempos definidos en los ANS aplicables, utilizando elementos originales, nuevos, no reacondicionados y de características iguales o superiores. Asimismo, deberá incluir transporte, instalación, configuración, licenciamiento, migración, pruebas, estabilización y actualización de inventarios y documentación técnica. La pérdida de vigencia, insuficiencia o terminación del licenciamiento, las suscripciones, la garantía o el soporte empresarial de fabricante no podrá invocarse como causal de indisponibilidad, reducción funcional, sobrecosto o incumplimiento de los niveles de servicio. El PROVEEDOR mantendrá la responsabilidad integral sobre la arquitectura ofertada durante toda la vigencia contractual. Independientemente de que la solución ofertada corresponda a una arquitectura de único fabricante o a una arquitectura multivendor, el PROVEEDOR debe disponer durante toda la ejecución contractual del personal especializado necesario para implementar, administrar, operar, integrar, monitorear y soportar cada uno de los servicios y componentes tecnológicos incluidos en su oferta. El equipo asignado deberá acreditar formación, experiencia y certificaciones técnicas vigentes del fabricante de las soluciones efectivamente ofertadas, o certificaciones equivalentes que demuestren las mismas competencias funcionales para el rol correspondiente. En arquitecturas multivendor, el PROVEEDOR debe garantizar cobertura especializada y certificada para cada fabricante, plataforma o componente que intervenga en la prestación de los servicios, así como personal con capacidad para gestionar su interoperabilidad e integración extremo a extremo. La utilización de aliados autorizados, filiales o personal certificado por diferentes fabricantes no limitará la responsabilidad integral del PROVEEDOR frente a la ENTIDAD. Este deberá garantizar la coordinación del equipo, el escalamiento oportuno con los fabricantes, la continuidad del soporte, la transferencia de conocimiento y el cumplimiento de los requisitos técnicos y niveles de servicio aplicables. Todas las certificaciones exigidas deberán permanecer vigentes durante la ejecución del contrato. En caso de pérdida de vigencia o indisponibilidad de un recurso, el PROVEEDOR debe asignar, dentro de los plazos establecidos en el Anexo Técnico 6, un reemplazo que cumpla iguales o superiores requisitos de formación, experiencia y certificación.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

<table>
<tr>
<td>Requisitos generales</td>
<td>
Contratar la prestación de servicios gestionados de seguridad digital y ciberseguridad, que permitan la protección de datos e infraestructura de TI de la Fiscalía General de la Nación.

A continuación, se indican cuáles son los servicios solicitados:

<table>
<tr><th>ÍTEM</th><th>TABLA DE CONTENIDO</th></tr>
<tr><td>S1.</td><td>Servicio de Firewall de Próxima Generación (NGFW)

El servicio será operado por los perfiles descritos en el Anexo Técnico 6 — Perfiles Profesionales, numeral P3 (Perfiles técnicos de Seguridad).</td></tr>
<tr><td>S2.</td><td>Servicio de WAF (Web Application Firewall) — Administración y Monitoreo (On-premise y Nube)</td></tr>
<tr><td>S3.</td><td>Servicio de Mitigación de Denegación de Servicio — DDoS (On-premise y Nube)</td></tr>
<tr><td>S4.</td><td>Servicio de Detección de Amenazas en Redes Públicas (Vigilancia Digital / External Threat Intelligence)</td></tr>
<tr><td>S5.</td><td>Servicio de Correo Seguro (Protección de Correo Electrónico Basada en Nube)</td></tr>
<tr><td>S6.</td><td>Servicio de Identidad Segura / Web Browser (Navegador Web Seguro Gestionado)</td></tr>
<tr><td>S7.</td><td>Manejo de Logs Históricos</td></tr>
<tr><td>S8.</td><td>Servicio de Data Loss Prevention — DLP (On-premise y Nube)</td></tr>
<tr><td>S9.</td><td>Servicio de Centro de Operaciones de Seguridad — SOC
El servicio será operado por los perfiles descritos en el Anexo Técnico 6 — Perfiles Profesionales, numeral P3 (Perfiles técnicos de Seguridad).</td></tr>
<tr><td>S10.</td><td>Plataforma SIEM (como parte del servicio SOC 24x7)</td></tr>
<tr><td>S11.</td><td>Plataforma SOAR (como parte del servicio SOC 24x7)</td></tr>
<tr><td>S12.</td><td>Servicio de Network Detection and Response (NDR)</td></tr>
<tr><td>S13.</td><td>Servicio de Administración del Network Access Control (NAC)</td></tr>
<tr><td>S14.</td><td>Servicio de Antimalware para Endpoint, Antimalware para servidores, Antimalware para NAS y XDR</td></tr>
<tr><td>S15.</td><td>Servicio de Detección de Malware (Día Cero y APTs) — On-premise y Nube — Integrado al SOC como Servicio</td></tr>
<tr><td>S16.</td><td>Servicio de seguridad en la Nube SASE</td></tr>
<tr><td>S17.</td><td>Servicio de Pruebas de Penetración
El servicio será operado por los perfiles descritos en el Anexo Técnico 6 — Perfiles Profesionales, numeral P3 (Perfiles técnicos de Seguridad).</td></tr>
<tr><td>S18.</td><td>Servicio de escaneo de Vulnerabilidades</td></tr>
<tr><td>S19.</td><td>Servicio de Pruebas de Penetración Persistente
El servicio será operado por los perfiles descritos en el Anexo Técnico 6 — Perfiles Profesionales, numeral P3 (Perfiles técnicos de Seguridad).</td></tr>
<tr><td>S20.</td><td>Servicio PAM (Privileged Access Management) Integrado con SOC, ITSM y Observabilidad</td></tr>
<tr><td>S21.</td><td>Servicio de Seguridad en IPV6</td></tr>
<tr><td>S22.</td><td>Servicio de Seguridad para SD-WAN Integrado con SOC, ITSM y Observabilidad</td></tr>
</table>
</td>
</tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	S23.	Servicio de administración de las herramientas de seguridad de Microsoft 365 integrado al SOC como servicio, Observabilidad e ITSM

Requisitos específicos

ÍTEM	TABLA DE CONTENIDO
S1.	Servicio de Firewall de Próxima Generación (NGFW) S1.1. Objeto, alcance y cobertura S1.1.1. El PROVEEDOR debe suministrar, implementar, operar y mantener un servicio gestionado de Firewall de Nueva Generación (NGFW) que incluya, como mínimo, los subservicios: seguridad perimetral, seguridad para tráfico de Internet (enfoque SSE/SASE), seguridad de tráfico de datos con detección y prevención de intrusos (IDS/IPS), VPN y ZTNA, Firewall Interno, antivirus perimetral y navegación segura. S1.1.2. El servicio debe cubrir la totalidad de las 876 sedes de la Fiscalía General de la Nación definidas en el Anexo Técnico 1.1 — Sedes, garantizando la protección de la totalidad de su tráfico. En todas las sedes la inspección del tráfico debe realizarse mediante componentes de inspección local, físicos o virtuales (incluido el NGFW virtualizado embebido en el CPE SD-WAN), dimensionados conforme a la categoría de cada sede. La plataforma del servicio y su administración podrán adoptar arquitecturas distribuidas, centralizadas o híbridas, conforme al diseño del PROVEEDOR aprobado por la ENTIDAD, sin que ello sustituya la capacidad de inspección local requerida en cada sede. S1.1.3. El servicio NGFW debe soportar despliegues en modalidad física y virtual, aplicables a entornos On-premise, nube pública Azure (actualmente implementado), Oracle OCI y otras nubes públicas que la ENTIDAD incorpore durante la ejecución del contrato, además nube privada y arquitecturas híbridas, garantizando cobertura de tráfico norte sur y este oeste, así como su integración con los sistemas institucionales de seguridad, gestión y observabilidad. El alcance incluye tanto escenarios actuales como futuras necesidades de expansión durante la vigencia del contrato. S1.1.4. El servicio debe prestarse durante treinta y seis (36) meses. S1.2. Modalidad del servicio y responsabilidades del PROVEEDOR S1.2.1. El servicio NGFW debe prestarse en modalidad administrada, incluyendo como mínimo: diseño, dimensionamiento, implementación, operación, monitoreo, afinamiento de políticas, gestión de cambios, soporte y mejora continua, con operación permanente conforme al esquema definido por la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S1.2.2. El PROVEEDOR debe realizar el dimensionamiento técnico (capacidad/throughput, inspección SSL/TLS, IPS, antimalware, HA, licenciamiento y suscripciones), y garantizar que la solución dimensionada sea suficiente para cumplir los ANS del servicio en sedes, datacenters y nubes. S1.2.3. Los requisitos técnicos se entenderán por capacidad funcional equivalente, demostrable mediante ficha técnica oficial, documentación del fabricante o pruebas de aceptación acordadas, sin exigir marcas o referencias exclusivas. S1.3. Capacidades mínimas NGFW — Seguridad perimetral y Firewall interno S1.3.1. El NGFW debe realizar inspección de tráfico a nivel de aplicación (L7/DPI) para soportar políticas basadas en aplicación y reducir evasiones por puertos/protocolos. S1.3.2. El NGFW debe identificar y controlar aplicaciones de forma granular (permitir/bloquear/limitar), con actualización periódica del catálogo de aplicaciones. S1.3.3. El PROVEEDOR debe implementar y operar Firewall Interno para segmentación y control de tráfico este-oeste (entre VLAN/zonas/segmentos), reduciendo movimiento lateral y aplicando políticas por origen/destino/servicio/aplicación. S1.3.4. El servicio debe registrar y auditar cambios de políticas, reglas, objetos y excepciones, habilitando trazabilidad para control contractual y auditoría. S1.4. Seguridad de tráfico de datos — IDS/IPS, antimalware y día cero S1.4.1. El servicio debe incluir capacidades de detección y prevención de intrusos (IDS/IPS) integradas o equivalentes, para detectar y bloquear ataques contra vulnerabilidades conocidas en tiempo real. S1.4.2. El servicio debe incluir antimalware/antivirus para el tráfico inspeccionado, con acciones configurables (bloqueo, cuarentena o permitir con registro). S1.4.3. El servicio debe incluir capacidad de sandboxing para análisis de archivos/artefactos sospechosos en entorno aislado, orientado a detección de amenazas de día cero. S1.5. Seguridad para tráfico de Internet — Enfoque SSE/SASE + navegación segura S1.5.1. El PROVEEDOR debe prestar un servicio administrado de seguridad para el tráfico de Internet asociado a la navegación de usuarios bajo enfoque de perímetro extendido (on-premise y/o nube), consistente con un modelo SSE/SASE, aplicando políticas uniformes

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

para usuarios en sedes y usuarios remotos. El número mínimo de usuarios es de 1.000 con la posibilidad de aumentar a demanda de la ENTIDAD hasta 30.000.

S1.5.2. El servicio de seguridad para tráfico de Internet debe incluir capacidades equivalentes a: (i) control L3-L7 equivalente a NGFW/FWaaS, (ii) IPS, (iii) antimalware/antivirus para tráfico web, (iv) navegación segura tipo SWG (filtrado URL avanzado y control de aplicaciones), y (v) inspección SSL/TLS con administración centralizada de políticas.

El filtrado URL debe soportar categorización y recategorización con actualización continua/automatizada (heurística, analítica avanzada, IA/ML o equivalente), verificable mediante documentación del fabricante o pruebas de aceptación.

S1.5.3. El servicio debe incluir protección DNS (bloqueo por reputación, phishing, C2, DGA o equivalente), con registro y exportación al SIEM del SOC como servicio.

La protección DNS debe permitir la detección y bloqueo de amenazas asociadas a dominios maliciosos, infraestructura de comando y control, actividades anómalas de resolución DNS, generación dinámica de dominios (DGA), túneles DNS, exfiltración de información y otras amenazas equivalentes. Asimismo, debe soportar integración con fuentes de inteligencia de amenazas mediante estándares abiertos o mecanismos equivalentes y aplicar políticas de protección tanto a usuarios conectados a la red corporativa como a usuarios remotos o itinerantes.

S1.5.4. Nodos de prestación y alta disponibilidad (HA) — SSE/SASE

S1.5.4.1. El subservicio de seguridad para tráfico de Internet (SSE/SASE) debe operar en alta disponibilidad para el tráfico originado en:
a) Nivel Central Bogotá.
b) Sede Cali.
La prestación debe realizarse mediante puntos de control locales (físicos y/o virtuales) y mediante puntos de presencia (PoP) en nube del servicio SSE/SASE, según diseño aprobado por la ENTIDAD, garantizando continuidad de navegación ante fallas de componentes, enlaces o región, sin degradación crítica del servicio.

S1.5.4.2. La alta disponibilidad debe soportar arquitecturas activo-activo o mecanismos equivalentes del servicio (persistencia de sesión, conmutación transparente), con el objetivo de minimizar el impacto percibido por usuarios y aplicaciones.

S1.5.4.3. El PROVEEDOR debe aportar el licenciamiento, suscripciones y software necesarios para habilitar todas las funcionalidades exigidas durante toda la vigencia del contrato, incluyendo soporte del fabricante.

S1.5.5. Diseño, documentación y puesta en operación (SSE/SASE)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S1.5.5.1. El PROVEEDOR debe entregar documentación del diseño (alto y bajo nivel) y documento “as-built” de la solución implementada, incluyendo diagramas, flujos (usuarios sede, usuarios remotos, egress Bogotá, egress Cali), dependencias y matriz de componentes.

S1.5.5.2. El PROVEEDOR debe ejecutar la configuración, implementación y operación del subservicio SSE/SASE conforme a los requerimientos del presente documento, incluyendo plan de transición y estabilización.

S1.5.6. Capacidades funcionales mínimas (SSE/SASE)

S1.5.6.1. La solución debe soportar funciones de integración de red necesarias cuando el diseño lo requiera, tales como rutas estáticas y/o dinámicas, túneles (IPsec/GRE u otros equivalentes), e integración con la arquitectura de egress definida por la ENTIDAD.

S1.5.6.2. La solución debe realizar control y decisión de acceso con base en: fuente (IP/usuario/grupo/dispositivo), destino (IP/FQDN/URL/categoría), servicio, aplicación/categoría de aplicación y categoría de URL.

S1.5.6.3. La solución debe mantener registros de eventos de seguridad, uso de recursos y estadísticas de eventos/tráfico, y permitir su consulta y exportación.

S1.5.7. Autenticación y control por identidad (usuarios locales y remotos) — SSE/SASE

S1.5.7.1. La solución debe soportar autenticación de usuario y validación de autorizaciones contra políticas de seguridad antes del establecimiento de la sesión, con aplicación de políticas a nivel de aplicación.

S1.5.7.2. Para usuarios remotos, la solución debe soportar integración con ZTNA como componente de SSE, aplicando verificación explícita y privilegio mínimo por aplicación.

S1.5.7.3. La solución debe integrarse con el proveedor de identidad institucional (SAML/OIDC/LDAP/AD/EntraID u otro equivalente), para asociación confiable de identidad a eventos y políticas.

S1.5.8. Navegación segura (SWG) — Sedes y remotos (Agente y/o Túnel / Navegador Seguro)

S1.5.8.1. Para usuarios en sedes (Bogotá y Cali), la navegación segura debe aplicarse en el punto de egress definido (local y/o nube SSE/SWG), manteniendo políticas consistentes.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S1.5.8.2. Para usuarios remotos, la navegación segura debe aplicarse mediante:
a) Agente en endpoint administrado técnicamente por el PROVEEDOR con supervisión de la ENTIDAD, y/o
b) Túnel seguro (tunneling/forwarding) hacia la plataforma SWG, de forma que el tráfico web del usuario remoto pase por el punto de control del SWG para filtrado, control de aplicaciones, inspección SSL y registro.
c) Navegador Seguro.

S1.5.8.3. El SWG debe, como mínimo, incluir filtrado de URL, antimalware y control de aplicaciones, y podrá incluir DLP/CASB si está contemplado en el alcance general del proceso.

S1.5.9. Administración segura y actualizaciones (SSE/SASE)

S1.5.9.1. La administración debe realizarse mediante interfaz GUI web exclusivamente por HTTPS (TLS 1.2 o superior) y/o aplicación cliente, con control de roles (RBAC) y auditoría de cambios.

S1.5.9.2. La solución debe operar sobre versión soportada por el fabricante y mantenerse actualizada con parches de seguridad, bajo un plan de mantenimiento acordado con la ENTIDAD (ventanas de cambio, reversión y evidencias).

S1.5.9.3. El PROVEEDOR debe optimizar, depurar y documentar las políticas a implementar, entregando durante la implementación y manteniendo actualizada durante la ejecución del contrato la matriz de políticas, objetos, grupos y excepciones conforme defina la ENTIDAD.

S1.6. Local Internet Breakout por sede + coherencia SD-WAN / SSE

S1.6.1. El PROVEEDOR debe habilitar salida a Internet local por sede (local breakout), manteniendo inspección, filtrado en línea del tráfico de usuarios y aplicación de políticas en el punto de salida con, como mínimo: Firewall, IPS, antimalware, control de aplicaciones y análisis de amenazas mediante sandboxing, ya sea en sitio o mediante arquitectura híbrida, sin degradar los niveles de servicio establecidos.

S1.6.2. El servicio debe integrarse con la arquitectura institucional SD-WAN/SASE/SSE de tal manera que: (i) cuando el usuario esté dentro de la red corporativa, el tráfico curse por SD-WAN con inspección local definida; y (ii) cuando el usuario esté fuera, el tráfico curse por SSE/SASE conforme a la ficha técnica de seguridad.

S1.7. VPN y ZTNA (sedes, usuarios remotos y nubes)

S1.7.1. El servicio debe incluir VPN Site-to-Site para conexión segura entre sedes y hacia recursos en nube, con registro de eventos para el SOC como servicio.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S1.7.2. El servicio debe incluir VPN Remote Access (IPsec/SSL o equivalentes) para usuarios remotos, con políticas de conexión y autenticación reforzada. El PROVEEDOR debe implementar autenticación multifactor (MFA) para el acceso remoto conforme a las políticas institucionales y mediante integración con el proveedor de identidad definido por la ENTIDAD, garantizando el registro y envío de eventos al SOC como servicio. S1.7.3. El servicio debe soportar ZTNA como componente de SSE para acceso a aplicaciones, aplicando verificación explícita y mínimo privilegio por aplicación. S1.8. Inspección SSL/TLS y gestión de certificados S1.8.1. El servicio debe soportar e implementar inspección SSL/TLS para tráfico web HTTP/HTTPS y flujos definidos, de manera que IPS/antimalware/filtrado URL/control de aplicaciones operen sobre tráfico cifrado cuando aplique, con política basada en riesgo y excepciones controladas. S1.8.2. El PROVEEDOR debe proveer e implementar el esquema de certificados requerido para inspección SSL, incluyendo generación, despliegue, rotación, revocación y documentación operativa. S1.8.3. El despliegue de certificados a estaciones de trabajo debe realizarse mediante Directorio Activo administrado por la ENTIDAD (GPO) y/o MDM institucional (si aplica), con acompañamiento del PROVEEDOR y procedimiento de verificación y evidencia. S1.8.4. La inspección SSL/TLS debe cubrir como mínimo HTTP/HTTPS. Protocolos adicionales (IMAP/SMTP/POP3 y variantes cifradas) solo serán exigibles si hacen parte del alcance definido y efectivamente transitan por el punto de control del servicio, conforme al diseño aprobado. S1.8.5. Las excepciones a la inspección SSL/TLS procederán por razones técnicas y/o normativas (pinning, aplicaciones no inspeccionables, categorías sensibles), y deben documentarse y aprobarse a través de la herramienta ITSM de la ENTIDAD, con trazabilidad y justificación. S1.8.6. Las soluciones ofertadas deben demostrar capacidad para identificar y aplicar políticas de seguridad sobre protocolos modernos, incluyendo QUIC, HTTP/3 o equivalentes, garantizando la efectividad de funciones tales como control de aplicaciones, filtrado web, DLP, inspección de tráfico y demás controles definidos en el Anexo Técnico. S1.8.7. Las capacidades de inspección, protección y procesamiento de tráfico cifrado asociadas a los servicios SD-WAN, SSE/SASE, SWG, FWaaS y demás componentes que hagan parte de la solución deberán soportar protocolos y algoritmos criptográficos vigentes y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

seguros, incluyendo como mínimo compatibilidad con TLS 1.2 y capacidades para TLS 1.3 cuando corresponda.

S1.8.8. La solución debe permitir la definición y aplicación de políticas de seguridad orientadas al control de versiones de protocolos, algoritmos criptográficos y mecanismos de intercambio de claves, permitiendo restringir o deshabilitar aquellos que sean considerados inseguros, obsoletos o no autorizados por la ENTIDAD.

S1.8.9. La solución debe soportar protocolos criptográficos vigentes y mecanismos de actualización tecnológica que permitan la adopción futura de esquemas de criptografía poscuántica o mecanismos funcionalmente equivalentes cuando estos se encuentren soportados por el fabricante y resulten aplicables a la arquitectura institucional.

S1.8.10. La solución debe permitir la identificación de certificados próximos a vencer, la generación de alertas preventivas, el soporte para mecanismos automatizados de renovación cuando sean compatibles con la arquitectura propuesta y el registro auditable de las operaciones asociadas al ciclo de vida de los certificados.

S1.9. Servicios en nube: Azure, Oracle OCI y otras nubes

S1.9.1. El PROVEEDOR debe incluir la administración del firewall en nube existente o implementado en Microsoft Azure dentro del alcance del servicio NGFW, incluyendo su operación, monitoreo, hardening, gestión de cambios y evidencias, gestionando toda solicitud de cambio mediante ITSM institucional.

S1.9.2. El PROVEEDOR debe definir el detalle técnico de los controles de seguridad en su arquitectura propuesta, garantizando operación integrada y cumplimiento de los ANS.

S1.9.3. El servicio de seguridad en las nubes públicas debe incluir la administración de controles de seguridad nativos y/o complementarios, tales como firewalls virtuales, WAF, controles de red, telemetría, detección y respuesta, e integraciones con el SOC como servicio.

S1.9.4. Si la ENTIDAD incorpora otras nubes públicas durante la ejecución, el PROVEEDOR debe extender el servicio NGFW y sus integraciones (SOC como servicio/Herramienta ITSM institucional/Plataforma de Observabilidad) a dichas nubes sin afectar la operación, conforme al plan de transición acordado.

S1.9.5. Infraestructura NGFW en nube actualmente disponible en la ENTIDAD

La ENTIDAD cuenta actualmente con la siguiente infraestructura NGFW en nube:

Ubicada en la nube Azure:

- Cuatro (4) NGFW marca Fortinet, referencia FortiGATE, en alta disponibilidad dos (2) Norte – Sur y dos (2) Este - Oeste;

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		- Un (1) repositorio de Logs marca Fortinet, referencia FortiANALYZER; - Con licenciamiento hasta el 30 de enero de 2027. Las referencias a Fortinet, FortiGate y FortiAnalyzer corresponden exclusivamente a la identificación de la infraestructura actualmente disponible en la ENTIDAD y no constituyen una exigencia de marca para los componentes nuevos, alternativos o de reemplazo que proponga el OFERENTE. S1.9.6. Uso potestativo de la infraestructura existente A discreción del PROVEEDOR, los componentes actualmente disponibles en la ENTIDAD pueden ser utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación del servicio, siempre que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso. La decisión de utilizar o no la infraestructura existente es responsabilidad del PROVEEDOR, sin que ello releve el cumplimiento total del objeto contractual ni de los requisitos exigidos para el servicio NGFW. S1.9.7. Mantenimiento, soporte y garantía de los componentes existentes En caso de que el PROVEEDOR decida incorporar dentro de su arquitectura propuesta cualquiera de los componentes NGFW actualmente disponibles en la ENTIDAD, debe asumir durante toda la ejecución del contrato, y sin costo adicional para la ENTIDAD, como mínimo, las siguientes obligaciones respecto de dichos componentes: a) mantenimiento preventivo, correctivo y evolutivo que resulte aplicable; b) soporte técnico especializado; c) garantía y gestión de garantía frente al fabricante o canal autorizado, cuando corresponda; d) reposición de partes, reemplazo de componentes defectuosos, cuando aplique; e) licenciamiento, actualización, parcheo, administración, operación, revisión de estado operativo y demás actividades necesarias para asegurar su correcto funcionamiento durante toda la ejecución contractual. S1.9.8. Validación de vigencia tecnológica y estado de soporte El PROVEEDOR debe verificar y garantizar, previo a la puesta en marcha y durante la ejecución contractual, que los componentes utilizados dentro de la arquitectura propuesta ya sean existentes o suministrados por él, no se encuentren en estado de EOL (End of Life), EOS (End of Support) o condición equivalente que comprometa su soporte, mantenimiento, actualización, operación segura o continuidad durante la ejecución del contrato.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Dicha validación debe estar soportada documentalmente mediante evidencia del fabricante, canal autorizado o fuente oficial técnicamente verificable.

S1.9.9. Sustitución obligatoria por fin de vida

Si durante la ejecución del contrato cualquiera de los componentes incorporados a la solución entra en estado de EOL, EOS o condición equivalente, o si dicho estado se determina de forma sobreviniente, el PROVEEDOR debe, sin costo adicional para la ENTIDAD, realizar su sustitución por un componente nuevo de iguales o superiores características técnicas, funcionales, de capacidad, desempeño, disponibilidad y compatibilidad, garantizando la continuidad del servicio y la no afectación material de la operación.

La sustitución debe incluir, cuando aplique, la migración, configuración, puesta en funcionamiento, pruebas, estabilización y transferencia operativa necesarias para mantener la integridad, disponibilidad y trazabilidad del servicio.

S1.9.10. Condiciones del reemplazo

Todo reemplazo de componentes debe garantizar plena compatibilidad con la arquitectura propuesta, continuidad del servicio, integridad de la información, preservación de configuraciones, conectores, playbooks, evidencias, registros históricos y trazabilidad aplicable. El reemplazo no podrá ocasionar una interrupción injustificada del servicio ni una disminución de las capacidades exigidas por la ENTIDAD.

S1.9.11. Responsabilidad integral sobre la arquitectura propuesta

Independientemente de que el PROVEEDOR decida utilizar o no la infraestructura existente de la ENTIDAD, es de su exclusiva responsabilidad garantizar que la arquitectura propuesta cumpla con todos los requerimientos del presente proceso, incluidos los de capacidad, disponibilidad, seguridad, soporte, interoperabilidad, continuidad, retención, trazabilidad, auditabilidad y desempeño operativo. Adicionalmente proponer mejoras en caso de que apliquen.

S1.9.12. Evaluación de compatibilidad y dimensionamiento

Si el PROVEEDOR decide utilizar componentes actualmente disponibles en la ENTIDAD, debe validar y documentar su compatibilidad, dimensionamiento, capacidad útil, desempeño y vida útil remanente respecto de la arquitectura propuesta y de la carga operativa del servicio, sin que ello implique limitación o reducción del alcance requerido por la ENTIDAD.

S1.9.13. Transición sin afectación material

Toda incorporación, sustitución, actualización, migración o retiro de componentes del NGFW debe ejecutarse bajo procedimiento controlado, con gestión de riesgos, plan de reversión y evidencias,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

evitando afectación material de la operación del servicio, pérdida de eventos, pérdida de trazabilidad o indisponibilidad no autorizada.

S1.9.14. No utilización de la plataforma existente

Si el PROVEEDOR decide no utilizar la infraestructura NGFW existente de la ENTIDAD, ello no lo exonera del cumplimiento integral del objeto contractual ni de los niveles de servicio exigidos. En tal caso, el PROVEEDOR debe suministrar, implementar, soportar y operar por su cuenta y riesgo, y sin costo adicional para la ENTIDAD, todos los componentes de hardware, software, licenciamiento, respaldo, continuidad, seguridad e integración necesarios para garantizar capacidades iguales o superiores a las definidas por la ENTIDAD.

S1.9.15. Condición de componentes nuevos

Todos los componentes nuevos o de reemplazo que se suministren para garantizar la prestación del servicio deberán ser originales, nuevos, no reacondicionados, no remanufacturados, estar soportados por el fabricante y cumplir con las especificaciones técnicas, funcionales, de capacidad, seguridad y compatibilidad exigidas por la ENTIDAD.

S1.9.16. Riesgo a cargo del PROVEEDOR

La decisión del PROVEEDOR de utilizar o no la infraestructura existente de la ENTIDAD es de su exclusiva responsabilidad y no podrá ser invocada como causa de sobrecostos, mayores tiempos de implementación, restricciones técnicas, disminución funcional, incumplimiento de niveles de servicio o solicitud de reconocimiento económico adicional.

S1.10. Integración con el SOC como servicio (SIEM/SOAR)

S1.10.1. El PROVEEDOR debe suministrar los logs del NGFW al SIEM del SOC como servicio mediante Syslog (RFC5424 o equivalente) o conectores estándar, garantizando continuidad de ingesta. Las capacidades del NGFW y sus componentes de inteligencia de amenazas deberán integrarse de forma abierta, interoperable y multivendor con las plataformas del SOC y soluciones de terceros, mediante mecanismos estándar como Syslog RFC5424 o equivalente, APIs, webhooks, conectores estándar y STIX/TAXII o formatos equivalentes cuando aplique. No se exige que todos los componentes pertenezcan a un mismo fabricante, ni se aceptarán restricciones que generen dependencia tecnológica injustificada o degradación funcional en entornos multivendor.

Los registros deben incluir, como mínimo: identidad de usuario y/o cuenta y su correlación con el flujo/sesión, IP origen/destino, URL/categoría, aplicación, acción (permitir/bloquear/inspeccionar), razón/firma, severidad y marca temporal.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S1.10.2. El PROVEEDOR debe integrar el servicio con el/los directorios y/o proveedor(es) de identidad definidos por la ENTIDAD (AD/LDAP/IdP o equivalente) para habilitar la asociación confiable de identidad a eventos y políticas. S1.10.3. El PROVEEDOR debe implementar los mecanismos de conectividad necesarios (VPN Site-to-Site, enlaces privados, integración nativa cloud o equivalentes) para garantizar el envío seguro, continuo y confiable de logs, eventos y alertas hacia el SOC como servicio (SIEM/SOAR), utilizando protocolos y conectores estándar. S1.10.4. El PROVEEDOR debe implementar arquitecturas de recolección intermedia (colectores SIEM en nube pública o privada) para el envío de logs hacia el SOC como servicio, siempre que garantice el cumplimiento de los requisitos de seguridad, disponibilidad, integridad, trazabilidad y continuidad de la ingesta establecidos por la ENTIDAD. La infraestructura asociada a dichos componentes es responsabilidad del PROVEEDOR. S1.10.5. Las acciones de contención derivadas del NGFW deben ejecutarse bajo gobernanza del SOC como servicio (playbooks/runbooks), con automatización solo para escenarios preaprobados y con aprobación para acciones de alto impacto, registrando evidencias en el ITSM institucional. S1.10.6. El PROVEEDOR debe implementar la solución NGFW con consola unificada para la administración y gestión para todos los firewalls que hagan parte del servicio (Nube/premisa). Nota: La consola unificada deberá permitir la administración centralizada de los componentes NGFW de la solución ofertada. Cuando las funciones SD-WAN y NGFW de las sedes sean prestadas por una misma plataforma, su administración deberá realizarse desde la misma consola, incluidas políticas, objetos, actualizaciones y registros. Cuando sean prestadas por fabricantes distintos, será suficiente garantizar una gestión integrada y una visibilidad unificada de ambas funciones en el SOC y en la Plataforma de Observabilidad. Esta exigencia no se extiende a los demás servicios de seguridad del proceso. S1.11. ITSM institucional y trazabilidad ITIL S1.11.1. Toda alerta relevante, incidente, requerimiento o solicitud de cambio del servicio NGFW y del subservicio SSE/SASE debe gestionarse mediante la herramienta ITSM institucional como único “system of record” para ITIL (estados, SLA, aprobaciones, evidencias y cierre formal). El SOC como servicio debe crear/actualizar/cerrar tickets directamente mediante integración (API/conector), garantizando trazabilidad completa (categoría, severidad, tiempos, responsables, evidencias, causa raíz y cierre).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S1.11.2. El PROVEEDOR debe asegurar que la integración del SOC como servicio y la herramienta ITSM institucional incluya, como mínimo: autenticación segura, control de roles, bitácora/auditoría de acciones y sincronización de estados del ticket, sin costos adicionales durante la vigencia contractual.

S1.12. Integración con herramienta de Observabilidad

S1.12.1. El servicio debe integrarse con la herramienta de observabilidad de la ENTIDAD para intercambio de información y visibilidad operacional (salud de componentes, caídas de conectores, colas/pipelines de ingesta, eventos operativos), conforme defina la ENTIDAD.

Retención de logs e integridad

S1.12.2. El PROVEEDOR debe garantizar retención mínima de logs por treinta y seis (36) meses en el repositorio primario definido (SOC/MDR o el que indique la ENTIDAD), asegurando: integridad (inmutabilidad o control equivalente), disponibilidad/consulta, RBAC/segregación, exportación en formatos estándar, soporte de cadena de custodia, respaldo y continuidad.

S1.13. Alta disponibilidad, continuidad y mantenimiento

S1.13.1. El PROVEEDOR debe diseñar y operar el servicio NGFW en alta disponibilidad, soportando un esquema activo-activo demostrable (persistencia de sesión y conmutación transparente), para minimizar interrupciones y cumplir los ANS del servicio.

S1.13.2. El PROVEEDOR debe mantener el servicio en versiones soportadas y aplicar parches de seguridad bajo un plan de mantenimiento acordado (ventanas, reversión y evidencias).

S1.14. Entregables y pruebas de aceptación

S1.14.1. El PROVEEDOR debe entregar documentación de diseño (alto/bajo nivel) y “as-built” (sedes, egresos, nube Azure/OCI, flujos SD-WAN/SSE), incluyendo matriz de componentes.

S1.14.2. El PROVEEDOR debe ejecutar y documentar pruebas que evidencien: (i) inspección L3-L7, (ii) IPS operativo, (iii) navegación segura (URL/app control), (iv) inspección SSL/TLS y gestión de certificados, (v) envío de logs al SIEM, (vi) creación/actualización de ticket en ITSM con evidencias, (vii) integración con observabilidad, y (viii) failover/alta disponibilidad.

S1.14.3. Se entenderá cumplida la “integración operativa” del servicio NGFW y del subservicio SSE/SASE cuando el PROVEEDOR ejecute y documente, como mínimo, las siguientes verificaciones en ambiente acordado con la ENTIDAD, dejando evidencia técnica y trazabilidad:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S1.14.3.1. SIEM (SOC como servicio): Se evidencie el envío y recepción en el SIEM del SOC como servicio de eventos/logs generados por el NGFW y por el componente SSE/SWG, mediante Syslog (RFC5424 o equivalente) o conectores estándar, y que dichos registros incluyan, como mínimo: identidad de usuario/cuenta (cuando aplique) y correlación con flujo/sesión, IP origen/destino, URL/categoría, aplicación, acción (permitir/bloquear/inspeccionar), razón/firma, severidad y marca temporal.

S1.14.3.2. ITSM (system of record): Se evidencie la creación/actualización/cierre de tickets (incidente/requerimiento/cambio) en el ITSM institucional mediante integración (API/conector), garantizando trazabilidad completa (categoría, severidad, tiempos, responsables, evidencias, causa raíz y cierre).

S1.14.3.3. SOAR: Se evidencie la operación de la integración SOAR—ITSM con sincronización bidireccional (ID cruzado SIEM/SOAR ↔ ITSM, estados, severidad/prioridad, bitácora y evidencias) y mecanismos de confiabilidad como idempotencia (no duplicación), colas/reintentos y alertas por fallas de integración.

S1.14.3.4. Observabilidad: Se evidencie en la herramienta de observabilidad de la ENTIDAD la salud de componentes y conectores (incluyendo caídas de conectores y colas/pipelines de ingesta) y eventos operativos relevantes del servicio, conforme defina la ENTIDAD.

S1.14.3.5. Evidencia mínima exigida: (i) capturas/export de eventos en SIEM, (ii) tickets en ITSM con evidencias enlazadas, (iii) bitácora/auditoría de acciones (incluida la integración SOAR cuando aplique), y (iv) panel/dashboards en Observabilidad mostrando estado de conectores e ingesta.

S1.15. Seguridad IoT y OT (descubrimiento, clasificación y protección)

S1.15.1. El PROVEEDOR debe proveer capacidades para descubrir, identificar y clasificar dispositivos IoT y OT conectados a la red de la ENTIDAD, habilitando visibilidad y control para su segmentación y protección.

S1.15.2. El PROVEEDOR debe aplicar políticas de control (permitir, bloquear, limitar o alertar) sobre el tráfico de dispositivos IoT/OT según perfiles y niveles de riesgo definidos por la ENTIDAD, manteniendo trazabilidad y registro de eventos para su integración con el SOC como servicio.

S1.15.3. El PROVEEDOR debe proveer capacidades para el descubrimiento, identificación y clasificación de dispositivos IoT y OT presentes en la red de la ENTIDAD, incluyendo, pero sin limitarse a entornos ICS/SCADA, PLC, RTU, HMI, historians y dispositivos de

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

automatización industrial. La cantidad de dispositivos no se define previamente y debe ser gestionada mediante un modelo escalable acorde con la operación.

S1.16. Soporte IPv4 e IPv6

S1.16.1. El servicio NGFW debe soportar operación dual-stack IPv4 e IPv6 para los escenarios incluidos en el alcance (sedes, datacenters y nubes), incluyendo aplicación de políticas, inspección, registro y exportación de logs al SIEM del SOC como servicio.
S1.16.2. Los componentes SSE/SASE deberán operar en IPv4 desde el inicio del servicio. El soporte IPv6/dual-stack de dichos componentes se exigirá conforme al plan de adopción IPv6 de la ENTIDAD (S21) y a la hoja de ruta oficial documentada del fabricante; el OFERENTE declarará capacidades y fechas. La operación dual-stack del servicio NGFW se mantiene según S1.16.1. En todo caso, el PROVEEDOR deberá habilitar el soporte IPv6 en los componentes SSE/SASE en las fechas declaradas en su oferta o cuando la ENTIDAD lo requiera conforme al plan de adopción aprobado, lo que primero ocurra según la disponibilidad documentada del fabricante, sin costo adicional, garantizando la aplicación consistente de políticas, visibilidad, trazabilidad y exportación de eventos al SIEM del SOC como servicio.

S1.17. Servicio DHCP

S1.17.1. El PROVEEDOR debe habilitar y operar funciones DHCP (o capacidad equivalente) en los segmentos definidos, garantizando registros, trazabilidad y gestión de cambios mediante ITSM institucional.

S1.18. Modalidades de implementación y despliegue (hardware/virtual/nube) y resiliencia en virtualización

S1.18.1. El PROVEEDOR debe suministrar e implementar el servicio NGFW en los formatos requeridos por la ENTIDAD, conforme a la arquitectura y plan de despliegue aprobados, incluyendo como mínimo:
(i) appliance físico para centros de datos y/o perímetros de red donde aplique; (ii) instancias software/virtual para entornos virtualizados o nubes privadas cuando aplique; y
(iii) componentes nativos o equivalentes en nubes públicas (Azure, OCI y las que la ENTIDAD incorpore durante la ejecución contractual).

S1.18.2. Para sedes, el PROVEEDOR debe implementar el/los componentes de inspección y control conforme a la tipología de sede definida por la ENTIDAD (categoría/criticidad/consumo), garantizando el cumplimiento de los ANS y evitando diseños que degraden la operación o afecten la continuidad del servicio.

S1.18.3. Cuando se implemente NGFW virtualizado y/o en alta disponibilidad, el PROVEEDOR debe garantizar que la arquitectura evite puntos únicos de falla y asegure segregación operacional de los

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

componentes redundantes (anti-affinity, dominios de falla independientes, zonas/regiones distintas cuando aplique o control equivalente), de tal forma que la virtualización no comprometa la resiliencia del servicio. Lo anterior deberá evidenciarse mediante documentación del diseño y pruebas de aceptación, incluyendo escenarios de falla y conmutación.

S1.19. Reportes operativos y ejecutivos

S1.19.1. El PROVEEDOR debe generar y entregar reportes operativos del servicio NGFW, como mínimo con periodicidad mensual, incluyendo: disponibilidad, capacidad/throughput, eventos relevantes, incidentes, cambios ejecutados, top de políticas/aplicaciones/URLs, y estado de integraciones (SIEM/ITSM/Observabilidad).

S1.19.2. El PROVEEDOR debe generar y entregar reportes ejecutivos, como mínimo con periodicidad trimestral, incluyendo: tendencias de riesgo, indicadores agregados, hallazgos relevantes y plan de mejora continua.

S1.20. DLP asociado a navegación/Internet

S1.20.1. El PROVEEDOR debe habilitar capacidades de DLP para el tráfico de navegación/Internet bajo el enfoque SSE/SASE, o integrar el servicio NGFW/SSE con el servicio DLP contratado, garantizando aplicación de políticas y generación de eventos para el SOC como servicio.

S1.20.2. Los eventos DLP generados deben ser exportados al SIEM del SOC como servicio y gestionados mediante el ITSM institucional, conforme a los procedimientos definidos por la ENTIDAD.

S1.21. Capacidades avanzadas de inspección y soporte forense

S1.21.1. La solución debe permitir obtención de evidencia forense asociada a políticas/reglas, mediante captura de paquetes (PCAP) o un mecanismo equivalente (trazas detalladas de sesión, exportación de flujos, logs enriquecidos), para exportación y análisis, preservando integridad y trazabilidad.

S1.21.2. La solución debe soportar control y visibilidad sobre tráfico SSH saliente (detección, bloqueo por política, registro), y cuando el fabricante lo soporte y el diseño lo contemple, podrá incluir inspección profunda en puertos configurables definidos por la ENTIDAD, registrando eventos asociados.

S1.22. Integración con detección de APT y malware día cero

S1.22.1. La solución debe integrarse con capacidad de detección de APT y malware día cero prevista en el proceso (sandbox/ATP) del Servicio de Detección de Malware (Día Cero y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

APTs), sin desarrollos a la medida, para inspección/detección en HTTP/HTTPS y otros protocolos definidos en el diseño aprobado.

S1.23. Capacidad mínima y escalamiento

S1.23.1. La solución debe licenciarse para soportar mínimo 1.000 usuarios, pero permitir un crecimiento futuro hasta 30.000 usuarios.

S1.23.2. El PROVEEDOR debe garantizar escalabilidad futura mediante: (i) margen de ampliación incluido sin costo hasta umbral cuantificado, o (ii) esquema de precios unitarios fijos de ampliación durante la vigencia contractual.

S1.23.3. El servicio debe demostrar capacidad de procesamiento mediante métricas estándar, verificables por ficha técnica oficial, documentación técnica o pruebas acordadas con la ENTIDAD, incluyendo como mínimo:
a) Throughput inspeccionado para tráfico HTTP/HTTPS con TLS inspection, cuando aplique, por cada sede, egress o PoP aplicable.
b) Transacciones por segundo (TPS), conexiones por segundo (CPS) o métrica equivalente del fabricante para SWG/IPS o componente de inspección aplicable.
c) Usuarios concurrentes soportados y/o número de endpoints con agente, cuando aplique.
d) El OFERENTE debe declarar la latencia añadida promedio y/o en percentil 95 de la solución propuesta, indicando la metodología de medición, perfil de tráfico, tamaño de paquetes, nivel de utilización, funcionalidades de seguridad habilitadas y condiciones de inspección SSL/TLS.

Este valor tendrá carácter técnico e informativo y será utilizado para verificar que la solución no genere degradación significativa sobre las aplicaciones y servicios institucionales. No será objeto de comparación directa entre ofertas cuando los resultados correspondan a metodologías diferentes.

El valor declarado deberá acreditarse mediante documentación técnica oficial del fabricante o pruebas de aceptación acordadas con la ENTIDAD, bajo condiciones representativas de la arquitectura implementada.

e) Modo de operación utilizado para la medición, funcionalidades de seguridad activas, proporción o alcance del tráfico cifrado inspeccionado cuando aplique, y condiciones generales de prueba.
Las métricas deberán corresponder a condiciones representativas de operación con las funcionalidades de seguridad requeridas habilitadas de forma concurrente. La ENTIDAD podrá solicitar evidencia técnica que permita validar que el valor ofertado corresponde al escenario documentado.

S1.23.4. La solución debe incluir reconocimiento/control de aplicaciones con catálogo actualizado automáticamente por el fabricante, incluyendo aplicaciones empresariales comunes. El

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		OFERENTE debe declarar el número total soportado, su método de actualización y evidencia oficial. S1.24. Plan de salida (Exit Plan) — NGFW/SSE/SASE S1.24.1. Al finalizar el contrato o ante terminación anticipada, el PROVEEDOR debe ejecutar un plan de salida que garantice continuidad del servicio y reversibilidad. Como mínimo, debe: (i) entregar exportación completa de configuración (políticas, reglas, objetos, perfiles, excepciones), inventario de componentes y conectores; (ii) entregar runbooks/procedimientos operativos, diagramas, "as-built" y evidencias de operación; (iii) entregar los registros (logs) conforme a la retención exigida, en formato explotable y con su correspondiente cadena de custodia; (iv) realizar transferencia de conocimiento y acompañamiento a la ENTIDAD o al nuevo proveedor; y (v) efectuar borrado seguro de información de la ENTIDAD en plataformas del PROVEEDOR, dejando acta y evidencia. S1.24.2. Tiempo de notificación del plan de salida: la ENTIDAD deberá notificar la terminación para la ejecución del plan de salida en los siguientes plazos, de acuerdo con las siguientes situaciones: a. Vencimiento normal del contrato: ciento veinte (120) días calendario. b. Migración o sustitución anticipada: noventa (90) días calendario. c. Evento sobreviniente o terminación inmediata: plazo contractual disponible.
	S2.	Servicio de WAF (Web Application Firewall) — Administración y Monitoreo (On-premise y Nube) S2.1. Objeto, alcance y cobertura S2.1.1. EL PROVEEDOR debe suministrar, implementar, operar, monitorear y mantener un servicio de WAF (Web Application Firewall) para la ENTIDAD, con cobertura en los centros de datos de la ENTIDAD (Bogotá y Cali) y en las nubes públicas que use la ENTIDAD, conforme a la arquitectura y plan de despliegue aprobados por la ENTIDAD. S2.1.2. EL PROVEEDOR debe asegurar la aplicación de políticas uniformes y trazables para los componentes on-premise y en nube, garantizando consistencia de configuración, operación, registro y gestión centralizada. S2.1.3. El servicio WAF debe implementarse bajo un modelo híbrido que integre la administración de los dispositivos existentes en la ENTIDAD (siempre y cuando sean utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación del servicio, y que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso) y con capacidades WAF en nube pública. El PROVEEDOR es

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

responsable del diseño y dimensionamiento técnico del servicio WAF, considerando la infraestructura disponible señalada en el numeral S2.2, los requisitos del proceso y la información validada durante la transición. El dimensionamiento deberá garantizar la suficiencia de la solución para cumplir los ANS y evitar la degradación crítica de las aplicaciones protegidas. La validación del inventario no releva al PROVEEDOR de esta responsabilidad ni genera, por sí sola, reconocimiento económico adicional.

S2.2. Infraestructura WAF actualmente disponible en la ENTIDAD

La ENTIDAD cuenta actualmente con la siguiente infraestructura WAF:
Ubicada en Bogotá:

- Dos (2) WAF marca Radware, modelo AppWall 1008;
- Con soporte y garantía hasta el 8 de junio de 2027.

Ubicada en Cali:

- Dos (2) WAF marca Radware, modelo AppWall 1008;
- Con soporte y garantía hasta el 8 de junio de 2027.

Ubicada en la nube Azure:

- Dos (2) WAF marca Fortinet, referencia FortiWEB;
- Con licenciamiento hasta el 30 de enero de 2027.

Ubicada en la nube OCI:

- Dos (2) WAF marca Fortinet, referencia FortiWEB;
- Con licenciamiento hasta el 30 de enero de 2027.

Las referencias a Radware, AppWall, Fortinet y FortiWEB corresponden exclusivamente a la identificación de la infraestructura actualmente disponible en la ENTIDAD y no constituyen una exigencia de marca para los componentes nuevos, alternativos o de reemplazo que proponga el OFERENTE.

S2.2.1. Uso potestativo de la infraestructura existente

A discreción del PROVEEDOR, los componentes actualmente disponibles en la ENTIDAD pueden ser utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación del servicio, siempre que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso.

La decisión de utilizar o no la infraestructura existente es responsabilidad del PROVEEDOR, sin que ello releve el cumplimiento total del objeto contractual ni de los requisitos exigidos para el servicio WAF.

S2.2.2. Mantenimiento, soporte y garantía de los componentes existentes

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		En caso de que el PROVEEDOR decida incorporar dentro de su arquitectura propuesta cualquiera de los componentes WAF actualmente disponibles en la ENTIDAD, debe asumir durante toda la ejecución del contrato, y sin costo adicional para la ENTIDAD, como mínimo, las siguientes obligaciones respecto de dichos componentes: a) mantenimiento preventivo, correctivo y evolutivo que resulte aplicable; b) soporte técnico especializado; c) garantía y gestión de garantía frente al fabricante o canal autorizado, cuando corresponda; d) reposición de partes, reemplazo de componentes defectuosos e) actualización, parcheo, administración, operación, revisión de estado operativo y demás actividades necesarias para asegurar su correcto funcionamiento durante toda la ejecución contractual. S2.2.3. Validación de vigencia tecnológica y estado de soporte El PROVEEDOR debe verificar y garantizar, previo a la puesta en marcha y durante la ejecución contractual, que los componentes utilizados dentro de la arquitectura propuesta ya sean existentes o suministrados por él, no se encuentren en estado de EOL (End of Life), EOS (End of Support) o condición equivalente que comprometa su soporte, mantenimiento, actualización, operación segura o continuidad durante la ejecución del contrato. Dicha validación debe estar soportada documentalmente mediante evidencia del fabricante, canal autorizado o fuente oficial técnicamente verificable. S2.2.4. Sustitución obligatoria por fin de vida Si durante la ejecución del contrato cualquiera de los componentes incorporados a la solución entra en estado de EOL, EOS o condición equivalente, o si dicho estado se determina de forma sobreviniente, el PROVEEDOR debe, sin costo adicional para la ENTIDAD, realizar su sustitución por un componente nuevo de iguales o superiores características técnicas, funcionales, de capacidad, desempeño, disponibilidad y compatibilidad, garantizando la continuidad del servicio y la no afectación material de la operación. La sustitución debe incluir, cuando aplique, la migración, configuración, puesta en funcionamiento, pruebas, estabilización y transferencia operativa necesarias para mantener la integridad, disponibilidad y trazabilidad del servicio. S2.2.5. Condiciones del reemplazo Todo reemplazo de componentes debe garantizar plena compatibilidad con la arquitectura propuesta, continuidad del servicio, integridad de la información, preservación de configuraciones, conectores, playbooks, evidencias, registros históricos y trazabilidad aplicable. El reemplazo no podrá ocasionar una interrupción injustificada del servicio ni una disminución de las capacidades exigidas por la ENTIDAD. S2.2.6. Responsabilidad integral sobre la arquitectura propuesta

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Independientemente de que el PROVEEDOR decida utilizar o no la infraestructura existente de la ENTIDAD, es de su exclusiva responsabilidad garantizar que la arquitectura propuesta cumpla con todos los requerimientos del presente proceso, incluidos los de capacidad, disponibilidad, seguridad, soporte, interoperabilidad, continuidad, retención, trazabilidad, auditabilidad y desempeño operativo.

S2.2.7. Evaluación de compatibilidad y dimensionamiento

Si el PROVEEDOR decide utilizar componentes actualmente disponibles en la ENTIDAD, debe validar y documentar su compatibilidad, dimensionamiento, capacidad útil, desempeño y vida útil remanente respecto de la arquitectura propuesta y de la carga operativa del servicio, sin que ello implique limitación o reducción del alcance requerido por la ENTIDAD.

S2.2.8. Transición sin afectación material

Toda incorporación, sustitución, actualización, migración o retiro de componentes del WAF debe ejecutarse bajo procedimiento controlado, con gestión de riesgos, plan de reversión y evidencias, evitando afectación material de la operación del servicio, pérdida de eventos, pérdida de trazabilidad o indisponibilidad no autorizada.

S2.2.9. No utilización de la plataforma existente

Si el PROVEEDOR decide no utilizar la infraestructura WAF existente de la ENTIDAD, ello no lo exonera del cumplimiento integral del objeto contractual ni de los niveles de servicio exigidos. En tal caso, el PROVEEDOR debe suministrar, implementar, soportar y operar por su cuenta y riesgo, y sin costo adicional para la ENTIDAD, todos los componentes de hardware, software, licenciamiento, respaldo, continuidad, seguridad e integración necesarios para garantizar capacidades iguales o superiores a las definidas por la ENTIDAD.

S2.2.10. Condición de componentes nuevos

Todos los componentes nuevos o de reemplazo que se suministren para garantizar la prestación del servicio deberán ser originales, nuevos, no reacondicionados, no remanufacturados, estar soportados por el fabricante y cumplir con las especificaciones técnicas, funcionales, de capacidad, seguridad y compatibilidad exigidas por la ENTIDAD.

S2.2.11. Riesgo a cargo del PROVEEDOR

La decisión del PROVEEDOR de utilizar o no la infraestructura existente de la ENTIDAD es de su exclusiva responsabilidad y no podrá ser invocada como causa de sobrecostos, mayores tiempos de implementación, restricciones técnicas, disminución funcional, incumplimiento de niveles de servicio o solicitud de reconocimiento económico adicional.

S2.3. Modalidad del servicio y responsabilidades del PROVEEDOR

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S2.3.1. El servicio WAF se presta en modalidad administrada e incluye, como mínimo: diseño y dimensionamiento, implementación, operación, monitoreo, afinamiento de políticas, gestión de cambios, soporte, mantenimiento y mejora continua, conforme al esquema definido por la ENTIDAD.

S2.3.2. EL PROVEEDOR asume el dimensionamiento técnico del servicio (capacidad/throughput, inspección/descifrado SSL/TLS cuando aplique, alta disponibilidad, licenciamiento y suscripciones), garantizando suficiencia para cumplir los ANS y no degradar la operación de las aplicaciones protegidas.

S2.4. Arquitectura e infraestructura (on-premise y nube)

S2.4.1. EL PROVEEDOR debe instalar y operar componentes WAF en los centros de datos de la ENTIDAD en Bogotá y Cali y, adicionalmente, habilitar el componente WAF en las nubes públicas que use la ENTIDAD, manteniendo un modelo híbrido coherente (on-premise y nube).

S2.4.2. El PROVEEDOR debe incluir la administración del WAF en nube existente o implementado en Microsoft Azure, Oracle OCI y otras nubes dentro del alcance del servicio WAF, incluyendo su operación, monitoreo, hardening, gestión de cambios y evidencias, gestionando toda solicitud de cambio mediante ITSM institucional.

S2.4.3. Para los centros de datos, el servicio WAF se presta mediante componentes físicos, con capacidad de inspección acorde con los requerimientos de desempeño de la ENTIDAD. La solución puede apoyarse en servicios de inteligencia de amenazas, reputación, analítica avanzada, protección de bots, firmas dinámicas u otras capacidades equivalentes provistas por el fabricante o integradas en la arquitectura ofertada, siempre que se garantice la continuidad operativa, el cumplimiento de los ANS y la no afectación del rendimiento de las aplicaciones protegidas.

S2.4.4. EL PROVEEDOR debe integrar el servicio con una consola de gestión centralizada que permita un panel único (single pane of glass) para supervisar y administrar tanto los dispositivos locales como los servicios en la nube.

S2.4.5. Si durante la ejecución contractual la ENTIDAD incorpora otras nubes públicas, el PROVEEDOR deberá extender el servicio WAF y sus integraciones con el SOC como servicio, la herramienta ITSM institucional y la plataforma de Observabilidad, mediante componentes o servicios WAF en nube que sean compatibles con el proveedor de nube incorporado y con la arquitectura ofertada.

Para efectos de dimensionamiento y comparabilidad de las ofertas, esta capacidad deberá contemplar inicialmente la protección de hasta cincuenta (50) aplicaciones y un throughput agregado de hasta cien (100) Mbps, sin afectar materialmente la operación y conforme al plan de transición acordado con la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

El OFERENTE no estará obligado a presentar certificación de compatibilidad respecto de proveedores de nube pública no definidos por la ENTIDAD al momento de la presentación de la oferta. Cuando se requiera la incorporación de una nueva nube, el PROVEEDOR deberá realizar la evaluación técnica de compatibilidad, presentar el diseño de integración, identificar los componentes y licenciamientos necesarios y ejecutar las correspondientes pruebas de aceptación.

Los crecimientos que superen los límites de cincuenta (50) aplicaciones o cien (100) Mbps se gestionarán mediante los precios unitarios, tramos de expansión o mecanismos económicos establecidos en el contrato, previa aprobación de la ENTIDAD.

Por fuera de la capacidad inicial señalada, la referencia a “otras nubes” no implica su incorporación automática ni ilimitada dentro del alcance y valor inicial del contrato; su inclusión deberá contar con solicitud formal de la ENTIDAD, dimensionamiento técnico previo y aprobación mediante los mecanismos contractuales aplicables, definiendo el alcance, las capacidades, el licenciamiento, los recursos, los plazos y las condiciones económicas correspondientes.

S2.5. Capacidades mínimas de inspección y protección

S2.5.1. El sistema debe tener capacidad de inspeccionar el tráfico de las aplicaciones protegidas en los puertos y protocolos publicados por la ENTIDAD, incluyendo tráfico cifrado mediante descifrado SSL/TLS cuando aplique.

S2.5.2. El servicio debe ofrecer protección avanzada de capa 7, incluyendo inspección profunda de contenidos para identificar y bloquear amenazas web conocidas y vulnerabilidades de día cero.

S2.5.3. EL PROVEEDOR debe proveer actualización continua de inteligencia (feeds) de amenazas para bloqueo de dominios, IPs y URLs maliciosas, sin costo adicional durante la vigencia contractual.

S2.5.4. La solución WAF, tanto para ambientes on-premise como nube, debe incorporar capacidades avanzadas de protección de APIs y gestión de automatización maliciosa (Bot Management), incluyendo como mínimo descubrimiento continuo de APIs, clasificación y diferenciación de tráfico automatizado legítimo y no legítimo, detección de comportamientos anómalos, mecanismos orientados a la mitigación de ataques de lógica de negocio, análisis de comportamiento y capacidades de integración con los servicios institucionales de SOC, SIEM/SOAR, ITSM y Observabilidad. El dimensionamiento definitivo de dichas capacidades debe realizarse de acuerdo con la línea base institucional y la arquitectura propuesta por el OFERENTE.

S2.6. Políticas adaptables, identidad y contexto

S2.6.1. El servicio debe permitir implementar políticas de seguridad basadas en identidad de usuario y contexto (dispositivo, ubicación y postura de seguridad), cuando aplique conforme al diseño aprobado por la ENTIDAD, con trazabilidad y auditoría de cambios.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S2.6.2. EL PROVEEDOR debe habilitar control de acceso basado en identidad y verificación continua de confianza de usuarios/dispositivos antes de permitir el acceso a las aplicaciones protegidas, cuando aplique conforme a la arquitectura definida. S2.7. DLP asociado a aplicaciones web (integración) S2.7.1. EL PROVEEDOR debe integrar funciones de DLP en el servicio WAF o integrar el WAF con el servicio DLP contratado, para garantizar visibilidad y control sobre datos confidenciales que residan o transiten por las aplicaciones web, según el alcance definido por la ENTIDAD. S2.8. Análisis y respuesta S2.8.1. El servicio de WAF debe soportar análisis contextual y modelos estadísticos o capacidades equivalentes para acelerar la investigación y corrección de amenazas en tiempo real, y facilitar el afinamiento de políticas para reducir falsos positivos sin disminuir el nivel de protección. S2.9. Soporte multi-entorno y políticas uniformes S2.9.1. El servicio debe permitir la aplicación de políticas uniformes en entornos híbridos (on-premises y nube), manteniendo consistencia operativa y de seguridad entre ambos entornos. S2.10. Administración segura, auditoría y mantenimiento S2.10.1. La administración del servicio WAF debe realizarse mediante interfaz GUI web por HTTPS (TLS 1.2 o superior) y/o aplicación cliente, con control de roles (RBAC) y auditoría de cambios. S2.10.2. EL PROVEEDOR debe mantener el servicio de WAF en versiones soportadas por el fabricante y aplicar parches de seguridad bajo un plan de mantenimiento acordado con la ENTIDAD, alineado con los lineamientos aplicables del Anexo Técnico 1 — Conectividad (requerimientos de mantenimiento). S2.11. Disponibilidad (ANS/SLA), rendimiento y compensaciones S2.11.1. EL PROVEEDOR debe comprometer un SLA de disponibilidad del servicio WAF, medido y verificado conforme al numeral S.17 del Anexo Técnico 5 — Acuerdo de Niveles de Servicio. S2.11.2. EL PROVEEDOR debe garantizar que los controles de seguridad no comprometan el rendimiento ni la experiencia del usuario final, y debe evidenciarlo mediante pruebas de aceptación y métricas definidas por la ENTIDAD (latencia añadida, tasa de errores, disponibilidad). S2.11.3. EL PROVEEDOR debe aplicar un esquema de compensaciones económicas (garantía financiera en SLAs) por

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

incumplimiento de los ANS/SLA del servicio WAF, en los términos que defina la ENTIDAD en el contrato y/o anexos de niveles de servicio.

S2.12. Integraciones con SOC como servicio (SIEM/SOAR), herramienta de Observabilidad de la ENTIDAD e ITSM institucional

S2.12.1. EL PROVEEDOR debe suministrar al SOC como servicio los logs, eventos y alertas de seguridad generados por el servicio WAF, mediante Syslog (RFC5424 o equivalente) y/o conectores estándar, garantizando continuidad de la ingesta, normalización y disponibilidad de consulta conforme a los procedimientos del SOC.

S2.12.2. Los registros enviados al SOC como servicio deben permitir trazabilidad para investigación y respuesta, e incluir como mínimo: identificación del activo WAF, aplicación/virtual host (cuando aplique), IP origen/destino, URL/recurso, método, acción ejecutada (permitir/bloquear/desafiar), regla/firma/categoría, severidad y marca temporal sincronizada.

S2.12.3. EL PROVEEDOR debe integrar el servicio WAF con la herramienta de Observabilidad de la ENTIDAD para intercambio de información y visibilidad operacional, incluyendo como mínimo: salud de componentes, disponibilidad/uptime, estado de HA/failover, consumo de recursos, caídas de conectores, colas/pipelines de ingesta (cuando aplique) y eventos operativos relevantes, conforme defina la ENTIDAD.

S2.12.4. Toda alerta relevante, incidente, requerimiento o solicitud de cambio asociada al servicio WAF (on-premise y nube) debe gestionarse mediante la herramienta ITSM institucional como único “system of record” (estados, SLA/ANS, aprobaciones, evidencias y cierre formal).

S2.12.5. EL PROVEEDOR debe asegurar que las integraciones con SOC como servicio, con ITSM y con Observabilidad incluyan mecanismos de autenticación segura, control de roles, bitácora/auditoría de acciones e indicadores de disponibilidad de conectores y sincronización de estados del ticket, sin costos adicionales durante la vigencia contractual.

S2.13. Soberanía y residencia de datos

S2.13.1. EL PROVEEDOR debe cumplir con las normas aplicables de protección de datos y con los lineamientos de soberanía y residencia de datos definidos por la ENTIDAD, respecto del almacenamiento y tratamiento de registros, evidencias y telemetría del servicio WAF.

S2.14. Integración funcional y consistencia del servicio

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S2.14.1. EL PROVEEDOR debe garantizar que los servicios de seguridad asociados al WAF se encuentren plenamente integrados en términos de operación, visibilidad, correlación de eventos y administración centralizada, evitando fragmentación operativa que impida la trazabilidad o el control contractual del servicio.

S2.15. Reportes del servicio WAF

S2.15.1. El PROVEEDOR debe entregar, como mínimo:
a) Reporte operativo mensual: disponibilidad/uptime, capacidad/throughput, latencia p95, tasa de errores, eventos relevantes, ataques mitigados/bloqueados, top reglas/falsos positivos, cambios ejecutados (con rollback si aplica), estado de firmas/feeds, salud de HA y de conectores (SIEM/ITSM/Observabilidad) y cumplimiento de KPI/ANS.
b) Reporte ejecutivo trimestral: tendencias de riesgo, principales superficies y aplicaciones, indicadores agregados, cumplimiento SLA/ANS, hallazgos relevantes y plan de mejora continua.
c) Informe por incidente/evento significativo: línea de tiempo, impacto, evidencias, acciones ejecutadas, verificación de restablecimiento y lecciones aprendidas.

S2.16. Criterios y pruebas de aceptación

S2.16.1. Se entenderá cumplida la integración operativa del servicio WAF cuando el PROVEEDOR ejecute y documente pruebas que evidencien: (i) recepción en SIEM del SOC como servicio de eventos/logs del WAF (on-premise y nube) con los campos mínimos definidos; (ii) creación/actualización/cierre de tickets en el ITSM institucional ante alertas relevantes/incidentes/cambios del WAF (cuando aplique); (iii) visibilidad en la herramienta de Observabilidad de la salud de componentes, estado HA/failover, disponibilidad/uptime y estado de conectores y colas/pipelines de ingesta; (iv) auditoría de acciones y control de roles en integraciones, sin costos adicionales.
La evidencia mínima incluirá: export/capturas de eventos SIEM, tickets ITSM con evidencias enlazadas y paneles/dashboards de Observabilidad.

S2.16.2. El PROVEEDOR debe ejecutar y documentar:

1) Protección L7: demostración de detección/bloqueo (o mitigación) de ataques web representativos (inyección, traversal, XSS) en ambiente de pruebas autorizado, con evidencias en logs.
2) SSL/TLS (cuando aplique): evidencia de descifrado/inspección y correcto funcionamiento de certificados (instalación/rotación), y registro de excepciones autorizadas.
3) Consistencia híbrida: evidencia de políticas uniformes aplicadas en WAF on-premise y WAF en nube, con gestión centralizada.
4) SIEM: verificación de envío/recepción de eventos al SOC (Syslog/conector) con campos mínimos y consulta exitosa.
5) ITSM: verificación de creación/actualización de ticket (incidente/cambio) con trazabilidad y evidencias.
6) Observabilidad: verificación de panel de salud (uptime, HA/failover, conectores, colas/pipelines) y alertas por caída de conectores.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		7) HA/failover (si aplica): simulación controlada de falla y evidencia de continuidad sin degradación crítica. 8) Rendimiento: medición de latencia añadida y tasa de errores bajo carga acordada (p95), evidenciando no degradación crítica. S2.17. Plan de salida – WAF Al finalizar el contrato o ante terminación anticipada, el PROVEEDOR debe ejecutar un plan de salida que garantice continuidad y auditabilidad. Como mínimo debe: (i) entregar exportación completa de configuración/políticas, reglas, objetos, perfiles y excepciones, así como la documentación "as-built" y runbooks; (ii) entregar inventario de componentes, conectores e integraciones (SIEM/SOAR/ITSM/Observabilidad) y evidencias de operación; (iii) entregar los registros, reportes y evidencias del servicio conforme a la retención definida por la ENTIDAD, en formato explotable; (iv) realizar transferencia de conocimiento y acompañamiento a la ENTIDAD o al nuevo proveedor; y (v) realizar borrado seguro de información de la ENTIDAD en plataformas del PROVEEDOR, dejando acta y evidencias.
	S3.	Servicio de Mitigación de Denegación de Servicio — DDoS (On-premise y Nube) S3.1. Objeto, alcance y cobertura S3.1.1. EL PROVEEDOR debe suministrar, implementar, operar, monitorear y mantener un servicio de mitigación de ataques de denegación de servicio (DDoS) para la Fiscalía General de la Nación, mediante tecnología de propósito específico que permita cumplir los ANS y características técnicas definidas en el presente proceso. S3.1.2. EL PROVEEDOR debe instalar e integrar componentes del servicio DDoS en los Datacenter de la ENTIDAD (Bogotá y Cali). Para las nubes públicas en uso por la ENTIDAD (Azure y OCI), la protección DDoS podrá acreditarse con los servicios nativos del proveedor de nube, complementados con el WAF y el NGFW desplegados en dichos ambientes, siempre que sea administrada por el PROVEEDOR, se integre al SOC y a la Plataforma de Observabilidad institucional y permita cumplir las capacidades de detección, mitigación, reporte y niveles de servicio exigidos. No se exigirá instalar componentes DDoS adicionales en cada nube; cuando la protección nativa no permita cumplir dichas capacidades, el PROVEEDOR deberá complementarla. S3.2. Capacidades mínimas de desempeño (dimensionamiento) S3.2.1. EL PROVEEDOR debe garantizar que la solución de mitigación DDoS cuente con una capacidad efectiva mínima de inspección y mitigación de ocho (8) Gbps, con posibilidad de escalar hasta veintiocho (28) Gbps, conforme al crecimiento del tráfico agregado bidireccional (entrada y salida) de la ENTIDAD y a su capacidad instalada actual y proyectada, sin degradación del servicio ni incumplimiento de los ANS. El cumplimiento de esta capacidad, incluida la capacidad de escalamiento hasta el valor indicado, debe acreditarse mediante documentación técnica oficial del fabricante y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

podrá ser validado mediante pruebas de aceptación, pruebas de desempeño o mecanismos de verificación técnica definidos por la ENTIDAD durante la implementación o ejecución contractual.

S3.2.2. EL PROVEEDOR debe garantizar que la solución de mitigación DDoS cuente con una capacidad efectiva inicial mínima de ocho millones (8.000.000) de paquetes por segundo (pps), con capacidad de escalamiento hasta veinticinco millones (25.000.000) de pps durante la ejecución contractual.

Estos valores corresponden a la capacidad agregada de la arquitectura integral del servicio de mitigación DDoS y no a una capacidad independiente por sitio, centro de datos, nube, componente o appliance. Lo anterior no limita la presentación de soluciones con capacidades superiores.

La solución debe atender las condiciones normales de operación y los escenarios de ataques DDoS de alta intensidad, incluidos aquellos que utilicen paquetes de tamaño mínimo, sin degradación del servicio ni incumplimiento de los ANS.

El OFERENTE debe declarar la capacidad inicial, la capacidad máxima, el mecanismo y tiempo de escalamiento, las condiciones de licenciamiento, las dependencias técnicas y la correlación entre el throughput en Gbps y la capacidad de procesamiento en pps, de acuerdo con la arquitectura propuesta.

El cumplimiento debe acreditarse mediante documentación técnica oficial del fabricante o proveedor del servicio y podrá verificarse mediante las pruebas de aceptación acordadas con la ENTIDAD, incluida la validación de la capacidad de escalamiento hasta el valor indicado.

S3.2.3. EL PROVEEDOR debe garantizar un tiempo de procesamiento de paquetes menor o igual a 70 microsegundos, verificable por ficha técnica oficial o pruebas de aceptación acordadas.

S3.3. Obligaciones funcionales del servicio

S3.3.1. EL PROVEEDOR debe garantizar mitigación de ataques en Capa 3 y 4 (protocolos/volumétricos) y en Capa 7 (aplicativos/HTTP Floods).

S3.3.2. EL PROVEEDOR debe garantizar protección de direcciones IP e infraestructura, así como de aplicaciones publicadas por nombre (FQDN), de manera que el servicio pueda proteger tanto aplicaciones web como infraestructura expuesta, conforme a la arquitectura definida por la ENTIDAD.

S3.3.3. EL PROVEEDOR debe garantizar detección automática de anomalías, con tiempos de identificación conforme a los niveles de servicio establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio, verificable.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S3.3.4. EL PROVEEDOR debe garantizar que la solución permita detectar y mitigar ataques DDoS desconocidos o de día cero mediante mecanismos basados en comportamiento, tales como líneas base adaptativas, análisis estadístico, técnicas heurísticas, aprendizaje automático o mecanismos funcionalmente equivalentes, permitiendo identificar desviaciones respecto del tráfico legítimo y aplicar acciones de mitigación sin afectar injustificadamente la disponibilidad de los servicios institucionales.

S3.3.5. EL PROVEEDOR debe entregar un reporte detallado posterior a cada evento mitigado (Post-Mortem), con información técnica suficiente para auditoría y lecciones aprendidas, conforme al formato definido por la ENTIDAD.

S3.4. Inspección SSL/TLS y control criptográfico

S3.4.1. EL PROVEEDOR debe garantizar capacidad de inspeccionar tráfico cifrado SSL/TLS sin degradar el rendimiento del servicio, realizando inspección profunda de paquetes (DPI) sobre tráfico cifrado, soportando como mínimo TLS 1.2 y TLS 1.3, incluyendo 0-RTT.

S3.4.2. EL PROVEEDOR debe soportar Encrypted Client Hello (ECH, RFC 9849) cuando aplique y sea técnicamente soportado por el componente que procese el tráfico TLS, sin que deba exigirse necesariamente al componente de mitigación DDoS. El OFERENTE debe declarar capacidades, limitaciones y políticas para tratar los flujos ECH cuando reduzcan la visibilidad necesaria.

S3.4.3. Para versiones anteriores (TLS 1.1 o inferiores), EL PROVEEDOR debe permitir definir políticas de bloqueo o inspección según los requerimientos de seguridad de la ENTIDAD, garantizando la mitigación de ataques sin degradar la latencia del servicio.

Nota: La capacidad de inspección de tráfico cifrado de los numerales S3.4.1 y S3.4.2 se mantiene como requisito de la arquitectura de seguridad ofertada y podrá acreditarse en el componente de mitigación DDoS o en los componentes que terminan TLS (WAF, NGFW, balanceador o proxy), siempre que estos se integren con el servicio DDoS y el SOC y garanticen una protección coordinada, trazable y sin brechas de responsabilidad.

S3.5. Disponibilidad del servicio (ANS/SLA)

S3.5.1. EL PROVEEDOR debe garantizar la disponibilidad (uptime) del servicio establecida en el numeral S.2 del Anexo Técnico 5 — Acuerdo de Niveles de Servicio, medida y verificada conforme a dicho anexo.

S3.6. Integraciones con SOC como servicio (SIEM/SOAR) y herramienta de Observabilidad de la ENTIDAD

S3.6.1. EL PROVEEDOR debe suministrar al SOC como servicio los logs, eventos y alertas de seguridad generados por el servicio DDoS

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		(incluyendo eventos de detección, inicio/fin de mitigación, tipo de ataque, vectores L3/L4/L7, acciones ejecutadas y resultado), mediante Syslog (RFC5424 o equivalente) y/o conectores estándar, garantizando continuidad de la ingesta y disponibilidad de consulta. S3.6.2. Los registros enviados al SOC como servicio deben permitir trazabilidad para investigación y respuesta, e incluir como mínimo: identificador del componente/ubicación (Bogotá, Cali o nube), activo o punto de mitigación, IP/FQDN protegido (cuando aplique), vector/capa (L3/L4/L7), métricas del evento (bps/pps cuando aplique), acción aplicada (bloquear/filtrar/desafiar/limitar), severidad, marca temporal sincronizada y referencia del evento para correlación. S3.6.3. EL PROVEEDOR debe integrar el servicio DDoS con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud de componentes, disponibilidad/uptime, estado de alta disponibilidad/failover, capacidad/uso (throughput y pps), latencia asociada a mitigación, estado de conectores hacia SOC/SIEM y eventos operativos relevantes, conforme defina la ENTIDAD. S3.6.4. EL PROVEEDOR debe asegurar que las integraciones con el SOC como servicio y con Observabilidad incluyan mecanismos de autenticación segura, control de roles, bitácora/auditoría de acciones y monitoreo de disponibilidad de conectores, sin costos adicionales durante la vigencia contractual. S3.7. Pruebas de aceptación de integraciones (SOC y Observabilidad) S3.7.1. En las pruebas de aceptación del servicio, EL PROVEEDOR debe evidenciar: (i) envío efectivo y continuo de eventos DDoS al SOC como servicio (SIEM/SOAR), (ii) visualización de métricas operacionales del servicio DDoS en la herramienta de Observabilidad, y (iii) comportamiento ante falla de conectores (alertamiento, recuperación y no pérdida crítica de eventos), conforme a los procedimientos definidos por la ENTIDAD.
	S4.	Servicio de Detección de Amenazas en Redes Públicas (Vigilancia Digital / External Threat Intelligence) S4.1. Objeto, alcance y cobertura S4.1.1. EL PROVEEDOR debe prestar un servicio administrado de detección de amenazas en redes públicas para la Fiscalía General de la Nación, orientado a identificar, alertar y apoyar la mitigación de exposiciones de marca, credenciales y activos digitales de la ENTIDAD en fuentes abiertas y no indexadas, con operación permanente (7x24). S4.2. Monitoreo de fuentes externas (detección) S4.2.1. EL PROVEEDOR debe monitorear fuentes externas para detectar suplantación y abuso de marca, incluyendo como mínimo: a) Detección de phishing y “squatting”: identificación de dominios fraudulentos que suplantan la marca institucional y el dominio fiscalia.gov.co.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

b) Monitoreo de Deep/Dark Web: búsqueda en foros, marketplaces y canales de mensajería utilizados por actores de amenaza para identificar credenciales filtradas asociadas a cuentas corporativas, bases de datos robadas y menciones de ataques planeados.
c) Protección de marca en redes sociales: detección de perfiles falsos en redes sociales públicas que utilicen signos distintivos de la ENTIDAD con fines fraudulentos.
d) Detección de fugas de información: monitoreo de repositorios y fuentes públicas (repositorios de código y sitios de publicación rápida) para identificar exposición de código fuente, llaves/API keys u otros artefactos o documentos sensibles de la ENTIDAD.

S4.3. Monitoreo multicanal y cobertura 7x24

S4.3.1. EL PROVEEDOR debe monitorear de forma exhaustiva y permanente (7x24) como mínimo:
a) Clear Web: motores de búsqueda, redes sociales, tiendas de aplicaciones y sitios de registro de dominios.
b) Deep/Dark Web: foros, marketplaces, canales de mensajería asociados a actores de amenazas y repositorios de código.

S4.4. Gestión de activos a vigilar (inventario y actualización)

S4.4.1. EL PROVEEDOR debe realizar, en conjunto con la ENTIDAD, la validación y afinamiento del inventario inicial de activos, dominios, palabras clave y elementos críticos a monitorear para el servicio de Threat Intelligence. Este inventario será dinámico y deberá mantenerse actualizado durante la ejecución del contrato, como insumo para la detección, correlación y análisis de amenazas.

S4.4.2. EL PROVEEDOR debe mantener actualizado, junto con la ENTIDAD, el inventario de “activos/keywords” a vigilar, incluyendo como mínimo: marcas, dominios, rangos de IP (IPv4 e IPv6) y nombres de proyectos sensibles definidos por la ENTIDAD.

S4.5. Detección y notificación de credenciales expuestas y uso anómalo de cuentas

S4.5.1. EL PROVEEDOR debe notificar en tiempo real cualquier filtración de cuentas corporativas de la ENTIDAD con credenciales asociadas, cuando dicha información sea identificada en las fuentes monitoreadas.

S4.5.2. EL PROVEEDOR debe notificar periódicamente hallazgos de cuentas corporativas vinculadas a categorías no autorizadas definidas por la ENTIDAD, de acuerdo con las políticas institucionales de uso aceptable.

S4.6. Gestión de “takedowns” y desmantelamiento (acciones de remoción)

S4.6.1. EL PROVEEDOR debe contar con capacidad legal y técnica para gestionar “takedowns” (solicitud de baja/eliminación) de sitios de phishing, perfiles falsos y aplicaciones móviles fraudulentas, ante registradores, ISPs y plataformas, según corresponda.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S4.6.2. EL PROVEEDOR debe realizar seguimiento diario a cada caso de remoción cuando no sea posible su baja inmediata, e informar el estado del ticket hasta su resolución final.

S4.7. Adquisición y preservación de evidencia

S4.7.1. EL PROVEEDOR debe capturar y preservar evidencia técnica antes de la eliminación/despublicación del activo malicioso (capturas de pantalla, cabeceras/headers y artefactos técnicos disponibles), para fines legales, forenses o de auditoría, conforme a los lineamientos que defina la ENTIDAD.

S4.8. Búsqueda retroactiva (línea base inicial)

S4.8.1. Con el inicio del contrato, EL PROVEEDOR debe realizar una búsqueda retroactiva mínima de seis (6) meses para identificar si existe información de la ENTIDAD expuesta o en circulación previa al inicio del servicio.

S4.9. Entrega de IoCs (Indicadores de Compromiso) e integración técnica (SIEM, SOAR y Observabilidad)

S4.9.1. EL PROVEEDOR debe entregar de forma automatizada (vía API y/o “feeds”) los IoCs detectados (IPs, URLs y hashes maliciosos) para su bloqueo o gestión en herramientas de seguridad de la ENTIDAD (firewall, EDR, proxy u otras), conforme al diseño de integración aprobado.

S4.9.2. EL PROVEEDOR debe disponer de integración vía API para que las alertas del servicio se enruten automáticamente al SOAR del SOC como servicio, conforme a los playbooks/runbooks definidos por la ENTIDAD.

S4.9.3. EL PROVEEDOR debe enviar al SIEM del SOC como servicio las alertas, eventos e IoCs generados por el servicio, mediante Syslog (RFC5424 o equivalente) y/o conectores estándar, garantizando continuidad de la ingesta, disponibilidad de consulta y trazabilidad para correlación.

S4.9.4. EL PROVEEDOR debe integrar el servicio con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud de conectores (API/feeds/Syslog o equivalentes), disponibilidad del servicio de monitoreo, colas/reintentos (cuando aplique), métricas operativas agregadas (volumen de hallazgos por fuente/categoría, tasas de envío de eventos, y estado de integraciones), conforme defina la ENTIDAD.

S4.10. Clasificación por riesgo y reportes

S4.10.1. EL PROVEEDOR debe clasificar cada hallazgo con un nivel de criticidad basado en impacto y probabilidad de ocurrencia, conforme al modelo definido por la ENTIDAD.

S4.10.2. EL PROVEEDOR debe entregar un informe mensual de tendencias que analice el panorama de amenazas relevante para

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

el sector y la marca Fiscalía General de la Nación, con hallazgos, métricas y recomendaciones.

S4.11. Cumplimiento normativo y confidencialidad

S4.11.1. EL PROVEEDOR debe garantizar que el monitoreo en Deep/Dark Web se realiza cumpliendo marcos legales aplicables y evitando interacción directa con actores de amenaza que pueda poner en riesgo a la ENTIDAD.

S4.11.2. EL PROVEEDOR debe asegurar confidencialidad estricta y manejo seguro de la información recolectada, especialmente cuando involucre credenciales, vulnerabilidades o hallazgos que puedan afectar la seguridad institucional, aplicando controles de acceso, registro de auditoría y mecanismos de protección de la información definidos por la ENTIDAD.

S4.12. Pruebas de aceptación del servicio

S4.12.1. EL PROVEEDOR debe ejecutar y documentar, dentro del plan de transición y estabilización, pruebas de aceptación acordadas con la ENTIDAD que evidencien como mínimo:
a) Monitoreo y detección multicanal (7x24): evidencia de cobertura y funcionamiento del monitoreo en Clear Web y Deep/Dark Web, conforme a las fuentes declaradas por el PROVEEDOR y los activos/keywords definidos por la ENTIDAD.
b) Detección de phishing y “squatting”: evidencia de detección y generación de alerta para un caso controlado asociado a fiscalia.gov.co, con clasificación de riesgo y evidencias mínimas del hallazgo.
c) Detección de credenciales expuestas: evidencia de notificación y registro de un hallazgo de credenciales corporativas (caso controlado o dataset de prueba), incluyendo criticidad y trazabilidad del evento.
d) Detección de fugas de información: evidencia de un hallazgo controlado asociado a exposición de artefactos sensibles (repositorio o publicación), con evidencia técnica mínima y clasificación de riesgo.
e) Gestión de “takedown” y seguimiento: evidencia de apertura, gestión y seguimiento de un caso controlado de remoción (sitio de phishing/perfil falso/aplicación fraudulenta), incluyendo radicación ante tercero, estado del ticket y registro de seguimiento hasta su cierre o decisión final.
f) Adquisición y preservación de evidencia: evidencia técnica del caso de remoción (capturas, cabeceras/headers y artefactos disponibles), preservada antes de la eliminación/despublicación, conforme a los lineamientos de la ENTIDAD.
g) Búsqueda retroactiva: entrega del informe de búsqueda retroactiva mínima de seis (6) meses con metodología y resultados, dentro del plazo de estabilización definido por la ENTIDAD.
h) Entrega automatizada de IoCs e integración técnica (SIEM, SOAR y campos mínimos): evidencia de entrega automatizada (API y/o feeds) de IoCs (IPs, URLs, hashes) y del envío de alertas/eventos al SIEM del SOC como servicio mediante Syslog (RFC5424 o equivalente) y/o conectores estándar; y, cuando aplique, enrutamiento de alertas al SOAR.
Adicionalmente, EL PROVEEDOR debe evidenciar en el SIEM la recepción de eventos representativos de los principales tipos de

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		hallazgo del servicio (phishing/squatting, credencial expuesta, fuga de información y caso de remoción/takedown), verificando que cada evento contiene los campos mínimos definidos en S4.13 (incluyendo, como mínimo: EventId, timestamp, Source/artefacto, FindingType, Asset/Keyword, IoCs, Severity/Criticality, ConfidenceScore cuando aplique, Evidence (referencia), mapeo ATT&CK cuando aplique, CaseStatus y Actions), mediante capturas/exportaciones del SIEM y/o evidencia documental del conector. i) Reporte mensual de tendencias: entrega del primer informe mensual de tendencias con contenidos mínimos, métricas de operación del servicio y recomendaciones. j) Integración con Observabilidad: evidencia de visualización en la herramienta de Observabilidad de la ENTIDAD de métricas operacionales e indicadores de salud del servicio e integraciones (estado de conectores, disponibilidad del servicio de monitoreo y métricas agregadas definidas), mediante capturas/exportaciones y/o evidencia documental. S4.12.2. EL PROVEEDOR debe consolidar los resultados de las pruebas de aceptación en un acta y un dossier de evidencias, con trazabilidad de cada caso de prueba, hallazgos, acciones realizadas, responsables y recomendaciones, conforme al procedimiento de aceptación que defina la ENTIDAD. S4.13. Campos mínimos de eventos para SIEM del SOC como servicio S4.13.1. EL PROVEEDOR debe garantizar que las alertas y eventos enviados al SIEM del SOC como servicio (por Syslog RFC5424 o equivalente y/o conectores estándar) sean explicables y trazables, permitiendo su correlación y análisis multi-fuente. S4.13.2. Los eventos/alertas enviadas al SIEM deben incluir, como mínimo, los siguientes campos (o su equivalente funcional en el formato del conector), sin perjuicio de campos adicionales del fabricante: a) Fecha/hora del evento con zona horaria y sincronización (timestamp). b) Fuente del evento (Source): origen del hallazgo (Clear Web / Deep-Dark Web / redes sociales / repositorio público) y el “artefacto” o entidad observada (dominio/URL, perfil, repositorio, publicación, credencial, base de datos referenciada), según aplique. c) Categoría del hallazgo (FindingType): phishing/squatting, perfil falso, fuga de información, credencial expuesta, mención de amenaza/ataque planeado, aplicación fraudulenta, u otra categoría definida por la ENTIDAD. d) Activo/keyword relacionado (Asset/Keyword): marca, dominio, proyecto sensible, rango IP u otro activo de vigilancia que generó el match, según inventario vigente. e) IoCs asociados (IoCs): dominios, IPs, URLs y hashes asociados al hallazgo, cuando existan, con su tipo y valor. S4.13.3. EL PROVEEDOR debe soportar la extracción, normalización y entrega/gestión de IoCs (hashes, dominios, IPs,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		URLs) y permitir su exportación en formatos estándar (STIX/TAXII o equivalente) para consumo por SIEM/SOAR/TIP cuando aplique.
	S5.	Servicio de Correo Seguro (Protección de Correo Electrónico Basada en Nube) S5.1. Objeto y alcance S5.1.1. EL PROVEEDOR debe proveer un servicio de protección de correo electrónico basado en nube para la totalidad de las cuentas de correo electrónico de la Fiscalía General de la Nación, incluyendo filtrado, detección, respuesta, capacitación/concienciación e integración con el SOC como servicio (SIEM/SOAR), las herramientas de Observabilidad e ITSM de la ENTIDAD, conforme al diseño aprobado por la ENTIDAD. S5.2. Condiciones técnicas de disponibilidad y operación S5.2.1. Modo de despliegue: EL PROVEEDOR debe implementar el servicio en un esquema que garantice alta protección del correo y que no introduzca una latencia superior a cinco (5) segundos en la entrega del correo legítimo, medida como el tiempo adicional atribuible al proceso de inspección/filtrado del servicio. El esquema de despliegue (arquitectura, flujos de enrutamiento y puntos de control) debe ser presentado por EL PROVEEDOR y aprobado por la ENTIDAD previo a su implementación. S5.2.2. El servicio de correo seguro debe cubrir todos los flujos de correo (interno–interno, interno–externo y externo–interno). La solución deberá garantizar la protección de los flujos de correo entrante, saliente e interno-interno. Para el flujo interno-interno, la cobertura podrá implementarse mediante gateway, integración por API, conectores nativos con la plataforma institucional de correo y colaboración o mecanismos funcionalmente equivalentes, siempre que se garanticen capacidades de detección, investigación, análisis retrospectivo, remediación posterior a la entrega, preservación de evidencias e integración con el servicio de SOC. S5.2.3. Alta disponibilidad: EL PROVEEDOR debe garantizar la disponibilidad (uptime) de la plataforma de filtrado/protección de correo establecida en el numeral S.4 del Anexo Técnico 5 — Acuerdo de Niveles de Servicio, medida y verificada conforme a dicho anexo. S5.2.4. Cobertura: EL PROVEEDOR debe garantizar cobertura de la totalidad de cuentas de correo activas de la ENTIDAD. El servicio debe abarcar el flujo de correo interno — externo, externo — interno e interno — interno. S5.2.5. Integración con identidad: EL PROVEEDOR debe integrar el servicio con el servicio de identidad institucional para que la aplicación de políticas de seguridad en correo se realice en función de usuarios y grupos, según el modelo definido por la ENTIDAD. S5.2.6. Enrutamiento y alta disponibilidad sobre SD-WAN: EL PROVEEDOR debe proveer el enrutamiento en alta disponibilidad requerido para el servicio de correo seguro a través del servicio de SD-WAN, conforme al diseño aprobado por la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S5.2.7. Continuidad del negocio (SPOOL): En caso de indisponibilidad del servicio de correo principal de la ENTIDAD, EL PROVEEDOR debe garantizar que el servicio de Correo Seguro sea capaz de almacenar/encolar los correos entrantes por un periodo mínimo de setenta y dos (72) horas, sin pérdida de datos, hasta el restablecimiento del servicio principal.

S5.3. Protección y respuesta

S5.3.1. Protección anti-phishing avanzada: EL PROVEEDOR debe incluir análisis de URLs en tiempo de clic (incluida reescritura/defensa de enlaces) y detección de suplantación de identidad (anti-spoofing/BEC) o capacidades equivalentes.

S5.3.2. Sandboxing de archivos: EL PROVEEDOR debe ejecutar adjuntos sospechosos en un entorno seguro (sandbox) antes de entregarlos al usuario.

S5.3.3. Cifrado extremo a extremo: EL PROVEEDOR debe habilitar capacidad de envío de correos cifrados automáticamente basados en el contenido, conforme a políticas definidas por la ENTIDAD.

S5.3.4. Autenticación de dominios: EL PROVEEDOR debe gestionar y monitorear registros SPF, DKIM y DMARC para reducir suplantación del dominio institucional y presentar informes mensuales de intentos de suplantación.

S5.3.5. Análisis de intención (IA): EL PROVEEDOR debe disponer de capacidad de detección de anomalías de lenguaje mediante parámetros preestablecidos y configurables, para apoyar la identificación de fraude/BEC.

S5.3.6. Remediación post-entrega (retrospección): EL PROVEEDOR debe contar con tecnología de retrospección para remediación post-entrega. Si un correo ya fue entregado y dentro de los diez (10) minutos siguientes se identifica como malicioso a nivel global, el sistema debe ejecutar la remoción automática del mensaje de los buzones afectados (cuando sea técnicamente posible) sin intervención manual, dejando trazabilidad del evento y de la acción ejecutada.

S5.3.7. Gestión de cuarentena (armonizada con ITSM — tickets automáticos)

S5.3.7.1.EL PROVEEDOR, a través del servicio de SOC Nivel 1 (L1) o esquema operativo definido por la ENTIDAD, debe gestionar la cuarentena institucional.

S5.3.7.2.Toda solicitud de liberación por posible falso positivo (iniciada por usuario autorizado mediante “add-in”/botón de reporte, o por administrador) debe generar automáticamente un ticket/caso en la herramienta ITSM institucional como único “system of record”. El ticket debe incluir como mínimo: clasificación, severidad/prioridad, identificación del mensaje (MessageId o equivalente), identificador de cuarentena, remitente/destinatario (conforme a política), fecha/hora,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		evidencia disponible, IoCs asociados cuando existan y justificación de la solicitud. S5.3.7.3. EL PROVEEDOR debe gestionar la liberación del correo en un tiempo máximo de treinta (30) minutos contados desde la creación/asignación del ticket en ITSM (según flujo definido por la ENTIDAD), siempre que la política y el análisis de seguridad lo permitan. La decisión (liberado/bloqueado/escalado) y sus evidencias deben quedar registradas en el ticket. S5.3.7.4.EL PROVEEDOR debe garantizar notificación al usuario destinatario y, cuando aplique conforme a políticas de la ENTIDAD, al remitente sobre la identificación/gestión del incidente, manteniendo registro de la actuación. S5.3.8. Sandboxing día cero: EL PROVEEDOR debe asegurar que archivos adjuntos con extensiones ejecutables, macros o comprimidos sean analizados en sandbox antes de su entrega definitiva. S5.4. Capacitación y concienciación S5.4.1. Simulacros de phishing: EL PROVEEDOR debe ejecutar, como mínimo, un (1) simulacro mensual dirigido a toda la ENTIDAD, variando temáticas conforme a un plan aprobado por la ENTIDAD. S5.4.2. Campañas educativas: EL PROVEEDOR debe desplegar automáticamente una cápsula educativa de máximo dos (2) minutos a todo usuario que haga clic en un enlace durante los simulacros y adicionalmente programar campañas educativas relacionadas con seguridad del correo con periodicidad trimestral durante la ejecución del contrato. S5.4.3. Reportes: EL PROVEEDOR debe entregar un reporte por cada simulacro mensual indicando como mínimo: población objetivo (usuarios a quienes aplicó), resultados y tipo de simulacro realizado; y debe entregar reporte de las campañas trimestrales ejecutadas. S5.4.4. Botón de reporte: EL PROVEEDOR debe suministrar e instalar un complemento (“add-in”) o botón de reporte en el cliente de correo de los usuarios, integrado directamente con el SOC como servicio para su análisis. S5.5. Inteligencia e integración (IoCs, SIEM/SOAR y protección VIP) S5.5.1. Alimentación de IoCs: EL PROVEEDOR debe exportar automáticamente al SIEM y al SOAR del SOC como servicio, como mínimo, los indicadores detectados en campañas/correos dirigidos a la ENTIDAD (direcciones IP, dominios/URLs y hashes de malware), garantizando continuidad de la ingesta y trazabilidad para correlación. S5.5.2. Integración SIEM/SOC: EL PROVEEDOR debe enviar eventos, alertas, veredictos (cuando aplique), IoCs y evidencias del servicio de Correo Seguro al SIEM del SOC como servicio mediante mecanismos soportados (API, Syslog RFC5424 o equivalente, webhook o conectores estándar), permitiendo correlación multi-fuente.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S5.5.3. Requisitos de explicabilidad y trazabilidad: EL PROVEEDOR debe garantizar que los eventos enviados al SIEM sean explicables y trazables (artefacto, fuente/origen, categoría/técnica cuando aplique, score/confianza cuando el fabricante lo soporte y evidencia asociada), sin exponer información sensible en claro.

S5.5.4. Integración SOAR: EL PROVEEDOR debe habilitar disparadores para playbooks SOAR asociados a incidentes de correo, de acuerdo con la gobernanza definida por la ENTIDAD (automático preaprobado o con aprobación).

S5.5.5. Formatos estándar de IoCs: EL PROVEEDOR debe soportar extracción, normalización y gestión de IoCs (hashes, dominios, IPs, URLs) y permitir exportación en formatos estándar (STIX/TAXII o equivalente) para consumo por SIEM/SOAR/TIP cuando aplique.

S5.5.6. Análisis de “impostores” (VIP): EL PROVEEDOR debe configurar reglas específicas para proteger a los usuarios VIP definidos por la ENTIDAD, detectando variaciones de caracteres (homógrafos y sustituciones) en nombres y/o direcciones de correo en mensajes externos.

S5.5.7. El PROVEEDOR debe implementar capacidades de protección de usuarios VIP bajo un modelo dinámico y escalable. La cantidad de perfiles VIP será definida y actualizada por la ENTIDAD durante la ejecución del contrato, sin establecerse un número fijo inicial, debiendo el PROVEEDOR garantizar la cobertura, monitoreo y protección conforme a los ANS establecidos.

S5.6. Integración con herramienta de Observabilidad de la ENTIDAD

S5.6.1. EL PROVEEDOR debe integrar el servicio de Correo Seguro con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud y disponibilidad del servicio, estado de conectores/integraciones (SIEM/SOAR/ITSM cuando aplique), colas/reintentos cuando aplique y métricas operativas agregadas (volumen de correos analizados, bloqueados, en cuarentena y remediaciones post-entrega ejecutadas), conforme defina la ENTIDAD.

S5.7. ITSM institucional (tickets automáticos y trazabilidad)

S5.7.1. EL PROVEEDOR debe integrar el servicio de Correo Seguro con la herramienta ITSM institucional, de modo que todo incidente/caso y eventos correlacionados que la ENTIDAD defina, genere automáticamente un ticket/caso en ITSM, incluyendo: clasificación, severidad, prioridad, asignación, evidencias, IoCs y trazabilidad.

S5.7.2. La integración ITSM debe soportar, como mínimo: creación automática de tickets, actualización automática del ticket con estados/evidencias, sincronización de estados (bidireccional cuando el ITSM lo permita) y trazabilidad completa de transacciones (éxito/fallo/reintentos/latencia).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S5.7.3. EL PROVEEDOR debe asegurar que el SOAR se integre con el ITSM institucional para: crear automáticamente tickets de Incidente y tareas asociadas, y cuando aplique, tickets de Cambio (incluido cambio de emergencia) y Problema; y sincronizar bidireccionalmente (ID cruzado SOAR/SIEM ↔ ITSM, estados, severidad/prioridad, bitácora y evidencias), garantizando idempotencia (no duplicación), colas/reintentos y alertas por fallas de integración.

S5.7.4. Si la ENTIDAD migra de ITSM durante la ejecución, EL PROVEEDOR debe adaptar la integración al nuevo ITSM en el plazo máximo definido contractualmente, sin afectar la operación 24x7, y soportar operación paralela si la ENTIDAD lo exige.

S5.8. Pruebas de aceptación del servicio

S5.8.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencien como mínimo:
a) Despliegue y operación del servicio para el universo de cuentas definido (mínimo 30.000), sin degradación crítica y cumpliendo la latencia máxima definida.
b) Alta disponibilidad y medición de uptime de la plataforma.
c) Spool/encolamiento de correo por mínimo 72 horas ante caída del servicio principal (prueba controlada).
d) Detección y bloqueo de phishing (incluido análisis en tiempo de clic) y suplantación/BEC (casos de prueba controlados).
e) Sandboxing de adjuntos y análisis de día cero (casos de prueba controlados).
f) Remediación post-entrega (retrospección) con remoción automática dentro del umbral definido (caso de prueba controlado).
g) Gestión de cuarentena con tickets automáticos ITSM y tiempos de atención establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio con trazabilidad y evidencias.
h) Integración SIEM/SOAR e IoCs: evidencia de exportación automatizada de IoCs (IPs, dominios/URLs y hashes) y de envío de eventos/alertas al SIEM del SOC como servicio, y cuando aplique, enrutamiento al SOAR con disparo de playbooks conforme a gobernanza; validando campos mínimos SIEM definidos en S5.9 mediante capturas/exportaciones del SIEM y/o evidencia documental del conector.
i) Integración ITSM (tickets automáticos): evidencia de creación automática de tickets en ITSM para los casos definidos por la ENTIDAD, incluyendo sincronización de estados/evidencias e ID cruzado (SIEM/SOAR ↔ ITSM) cuando aplique.
j) Integración con Observabilidad: evidencia de visualización en Observabilidad de métricas operacionales e indicadores de salud del servicio e integraciones (SIEM/SOAR/ITSM cuando aplique).

S5.8.2. EL PROVEEDOR debe consolidar resultados de pruebas en un acta y dossier de evidencias, conforme al procedimiento de aceptación definido por la ENTIDAD.

S5.9. Campos mínimos de eventos para SIEM (SOC como servicio)

S5.9.1. EL PROVEEDOR debe garantizar que las alertas y eventos enviados al SIEM del SOC como servicio sean explicables y trazables, permitiendo su correlación y análisis multi-fuente.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S5.9.2. Los eventos/alertas enviadas al SIEM deben incluir, como mínimo: EventId, timestamp, Source y categoría de amenaza, referencia de artefacto (MessageId o equivalente cuando aplique), IoCs, acción ejecutada, severidad/criticidad y racional. S5.9.3. EL PROVEEDOR debe asegurar que la exportación de IoCs soporte formatos estándar (STIX/TAXII o equivalente) cuando aplique, para consumo por SIEM/SOAR/TIP. NOTA: Durante la vigencia del contrato, LA ENTIDAD podrá sustituir o modificar la plataforma de correo electrónico institucional. En tal evento, EL PROVEEDOR debe adaptar y alinear el SERVICIO a la nueva plataforma, realizando las actividades de configuración, integración y/o migración que resulten necesarias, garantizando la continuidad del servicio y el cumplimiento de los acuerdos de nivel de servicio (ANS), sin costos adicionales para LA ENTIDAD.
	S6.	Servicio de Identidad Segura / Web Browser (Navegador Web Seguro Gestionado) S6.1. Objeto y alcance S6.1.1. EL PROVEEDOR debe suministrar, implementar, operar y mantener una solución de navegador web seguro (Web Browser) con identidad segura, orientada a habilitar el acceso controlado a las aplicaciones de la ENTIDAD, con sincronización obligatoria del perfil de usuario contra el Identity Provider (IdP) institucional y aplicación de políticas de seguridad por usuario/grupo, conforme al diseño aprobado por la ENTIDAD. S6.1.2. La solución de Browser Seguro debe integrarse con la arquitectura SSE/SASE propuesta y soportar mecanismos de acceso seguro a aplicaciones mediante ZTNA y controles de protección de datos basados en identidad, contexto y nivel de riesgo. Se aceptarán mecanismos funcionalmente equivalentes implementados mediante navegador seguro, CASB, DLP, aislamiento remoto del navegador, control de sesión u otros componentes de seguridad integrados, siempre que permitan aplicar políticas de acceso y protección de información, generar trazabilidad e integrarse con los servicios institucionales de seguridad. S6.2. Sincronización nativa con IdP (SSO) S6.2.1. EL PROVEEDOR debe garantizar que el navegador seguro permita la sincronización obligatoria del perfil de usuario con el IdP institucional mediante SAML u OIDC, de forma que la autenticación y el acceso a aplicaciones se gestione bajo el modelo de identidad definido por la ENTIDAD. S6.2.2. EL PROVEEDOR debe permitir que la ENTIDAD defina políticas basadas en identidad (usuario/grupo) para el acceso a aplicaciones y la aplicación de controles, conforme a la integración con el directorio/IdP institucional (Directorio Activo). S6.3. Aislamiento de sesión (segregación corporativa/personal)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S6.3.1. EL PROVEEDOR debe garantizar que la solución sea capaz de aislar las sesiones de las aplicaciones de la ENTIDAD de cualquier otra actividad de navegación personal del usuario en los equipos, manteniendo segregación de sesiones, datos y artefactos de navegación, conforme a la política de seguridad definida por la ENTIDAD.

S6.4. Extensiones forzadas (controles y “add-ins” de seguridad)

S6.4.1. La solución debe permitir la aplicación centralizada y persistente de controles de seguridad de navegación definidos por la ENTIDAD. Cuando la arquitectura propuesta lo requiera, dichos controles podrán implementarse mediante extensiones gestionadas del navegador; alternativamente, podrán implementarse mediante mecanismos equivalentes propios de la solución ofertada, tales como aislamiento remoto de navegación u otras tecnologías funcionalmente equivalentes.

S6.5. Aplicaciones legadas o no federadas con MFA

S6.5.1. Para las aplicaciones legadas, aplicaciones on-premise o aplicaciones que no soporten de forma nativa SAML, OIDC u otros protocolos modernos de federación de identidad, EL PROVEEDOR debe implementar mecanismos de intermediación segura que permitan incorporar controles de autenticación reforzada, autenticación multifactor, autorización basada en políticas e integración con el proveedor de identidad institucional, conforme al diseño aprobado por la ENTIDAD.

La capacidad podrá implementarse mediante navegador seguro, proxy de acceso, gateway de aplicaciones, ZTNA, reverse proxy, access broker u otros mecanismos funcionalmente equivalentes, sin exigir una denominación comercial, arquitectura o fabricante específico.

La solución deberá garantizar como mínimo:
1. Integración con el directorio y proveedor de identidad institucional.
2. Aplicación de MFA cuando sea requerido por la política.
3. Control de acceso por usuario, grupo, rol, dispositivo, aplicación, ubicación y nivel de riesgo.
4. Aplicación del principio de mínimo privilegio.
5. Registro y trazabilidad de autenticaciones, autorizaciones y sesiones.
6. Integración con SOC, SIEM, SOAR, ITSM y Observabilidad.
7. Gestión controlada de excepciones y accesos de emergencia.

El OFERENTE debe demostrar la capacidad mediante documentación técnica oficial y pruebas de aceptación acordadas con la ENTIDAD.

S6.5.2. Se aceptarán soluciones que proporcionen capacidades funcionalmente equivalentes que permitan aplicar mecanismos de autenticación reforzada, autenticación multifactor (MFA), control de acceso basado en políticas, integración con el proveedor de identidad institucional y trazabilidad de accesos sobre aplicaciones legadas o no federadas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S6.6. Definición y gestión de políticas

El PROVEEDOR debe garantizar que la solución tenga las siguientes capacidades:

S6.6.1. Permitir la definición, ajuste y aplicación de políticas adicionales a las reglas básicas predeterminadas, incluyendo políticas por usuario/grupo, por aplicación y por contexto, conforme a lo que defina la ENTIDAD.

S6.6.2. Aplicar controles de acceso seguro a aplicaciones corporativas conforme a la arquitectura Zero Trust definida por la ENTIDAD.

S6.6.3. Implementar controles granulares sobre acciones de los usuarios dentro del navegador, incluyendo restricciones de descarga, carga de archivos, impresión, copiar/pegar, captura de pantalla u otras acciones equivalentes cuando resulte aplicable.

S6.6.4. Aplicar políticas diferenciadas para el acceso a aplicaciones corporativas y personales.

S6.6.5. Reducir los riesgos de fuga de información mediante controles visuales, mecanismos de trazabilidad o funcionalidades equivalentes.

S6.6.6. Aplicar restricciones sobre transferencia de información y uso de recursos locales conforme a las políticas definidas por la ENTIDAD.

S6.7. Detección de accesos anómalos y respuesta

S6.7.1. EL PROVEEDOR debe disponer de capacidades para detectar comportamientos anómalos en inicios de sesión y uso de aplicaciones (intentos no habituales, sesiones duplicadas u otros comportamientos definidos por la ENTIDAD) y responder aplicando los bloqueos/controles necesarios conforme a las políticas aprobadas.

S6.8. Reportes y seguimiento

S6.8.1. EL PROVEEDOR debe entregar a la ENTIDAD un reporte mensual de accesos a las aplicaciones, incluyendo como mínimo: registros de acceso, ubicación (cuando aplique), usuario, aplicaciones accedidas, fecha y hora, y métricas operacionales relevantes definidas por la ENTIDAD, preservando la confidencialidad de la información.

S6.9. Implementación, pruebas, afinamiento y documentación

S6.9.1. EL PROVEEDOR debe realizar la instalación, pruebas y afinamiento del navegador seguro, y debe elaborar y entregar manuales/guías de instalación y operación para proveedores y usuarios de la ENTIDAD, conforme al alcance y lineamientos aprobados. El despliegue del navegador seguro podrá ejecutarse de manera gradual (por fases), conforme a un plan de implementación propuesto por el PROVEEDOR y aprobado por la ENTIDAD, garantizando pruebas, estabilización y cobertura total al término del despliegue.

S6.10. Cobertura funcional sobre aplicaciones institucionales

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S6.10.1. EL PROVEEDOR debe garantizar que el navegador seguro funcione con los accesos a las aplicaciones que disponga la ENTIDAD, conforme a inventario y priorización definidos por la ENTIDAD.

S6.10.2. En caso de modificación de las aplicaciones o incorporación de nuevas aplicaciones durante la ejecución contractual, EL PROVEEDOR debe realizar los ajustes necesarios de configuración e integración del navegador seguro sin costo adicional para la ENTIDAD, conforme al procedimiento de gestión de cambios aplicable.

S6.11. Integración con ITSM institucional (tickets automáticos, trazabilidad y CMDB)

S6.11.1. EL PROVEEDOR debe integrar el servicio de identidad segura / navegador web seguro con la herramienta ITSM de la ENTIDAD, de modo que todo incidente/caso y eventos correlacionados que la ENTIDAD defina genere automáticamente un ticket/caso en ITSM, incluyendo: clasificación, severidad, prioridad, asignación, evidencias e información de trazabilidad.

S6.11.2. La integración debe soportar, como mínimo: creación automática de tickets, actualización automática del ticket con estados/evidencias, sincronización de estados (bidireccional cuando el ITSM lo permita), trazabilidad completa de transacciones (éxito/fallo/reintentos/latencia) e idempotencia (no duplicación), incluyendo alertas por fallas de integración.

S6.11.3. La integración debe realizarse mediante mecanismos estándar soportados por el ITSM (APIs/servicios/webhooks o equivalentes), evitando requisitos direccionadores por marca.

S6.11.4. EL PROVEEDOR debe consumir la CMDB de la ENTIDAD para enriquecer eventos/alertas y tickets con criticidad, propietario, servicio relacionado, ambiente y metadatos del CI. Cada ticket debe quedar vinculado al CI correspondiente en CMDB, habilitando priorización automática y reportes por servicio/proceso.

S6.11.5. EL PROVEEDOR debe reportar hallazgos de inconsistencias CMDB (CI inexistente, atributos faltantes) como tickets de mejora/problema según el modelo ITSM de la ENTIDAD.

S6.12. Integración con SOC (SIEM/SOAR)

S6.12.1. EL PROVEEDOR debe habilitar el envío de eventos/alertas del servicio (autenticaciones, bloqueos, anomalías, cambios relevantes de política y eventos de los mecanismos de intermediación segura para aplicaciones legadas o no federadas cuando aplique) al SIEM del SOC como servicio mediante mecanismos soportados (API/syslog/webhook o conectores estándar), permitiendo correlación multi-fuente.

S6.12.2. EL PROVEEDOR debe habilitar disparadores para playbooks en el SOAR cuando aplique (contención por bloqueo de

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		sesión, revocación de sesión/credenciales u otras acciones definidas por la ENTIDAD), bajo gobernanza definida (automático preaprobado o con aprobación). S6.13. Integración con herramienta de Observabilidad de la ENTIDAD S6.13.1. EL PROVEEDOR debe integrar el servicio con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud del servicio, disponibilidad, estado de conectores/integraciones (IdP/SIEM/SOAR/ITSM cuando aplique), colas/reintentos y métricas operacionales agregadas definidas por la ENTIDAD. S6.14. Pruebas de aceptación S6.14.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencien como mínimo: a) Sincronización obligatoria con IdP (SAML/OIDC) y aplicación de políticas por usuario/grupo. b) Aislamiento efectivo de sesiones corporativas frente a navegación personal. c) Evidencia de aplicación efectiva, centralizada y persistente de los controles de seguridad de navegación definidos por la ENTIDAD, mediante el mecanismo propio de la arquitectura ofertada, incluyendo extensiones gestionadas, aislamiento remoto de navegación o mecanismos funcionalmente equivalentes. d) Operación del mecanismo de intermediación segura para aplicaciones legadas o no federadas con MFA (caso de prueba controlado). e) Detección de accesos anómalos y aplicación de controles/bloqueos conforme a políticas. f) Generación de reporte mensual con los campos mínimos definidos por la ENTIDAD. g) Evidencia de integraciones SOC: envío de eventos/alertas al SIEM y disparo/enrutamiento al SOAR cuando aplique, conforme a gobernanza definida. h) Evidencia de Observabilidad: visualización en la herramienta de Observabilidad de la ENTIDAD de métricas operacionales e indicadores de salud del servicio e integraciones (IdP/SIEM/SOAR/ITSM cuando aplique). S6.14.2. EL PROVEEDOR debe consolidar resultados de pruebas en un acta y dossier de evidencias, conforme al procedimiento de aceptación definido por la ENTIDAD.
	S7.	Manejo de Logs Históricos S7.1. Almacenamiento y acceso por parte de la ENTIDAD El PROVEEDOR debe garantizar el almacenamiento y la disponibilidad de la totalidad de los registros de eventos (logs) que se generen con ocasión de la implementación, administración, operación, monitoreo, gestión y soporte de todos los servicios contemplados en la presente ficha técnica, asegurando a la Fiscalía General de la

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Nación el acceso directo y permanente para consulta y exportación de dichos registros durante toda la vigencia del contrato.

S7.2. Retención mínima para analítica y retención histórica

El PROVEEDOR debe garantizar, como mínimo, los siguientes periodos de retención, en concordancia con la retención general de logs de treinta y seis (36) meses definida para los servicios de seguridad: a) Retención para analítica/consulta operativa: no inferior a treinta y seis (36) meses, con capacidad de búsqueda y exportación de los logs retenidos. b) Retención histórica: treinta y seis (36) meses adicionales en modo de datos fríos/archivado (cold/archive), asegurando disponibilidad para consulta o recuperación bajo requerimiento de la ENTIDAD y preservación de la información para fines de auditoría, investigación y uso probatorio, conforme a la retención diferenciada definida para el componente SIEM/SOC.

S7.3. Integridad, custodia y exportación controlada

El PROVEEDOR debe proteger los logs contra modificación o borrado no autorizado, mediante mecanismos verificables de integridad y custodia, preferiblemente con almacenamiento inmutable/WORM o controles equivalentes (hashing, control de borrado, segregación de funciones y auditoría de accesos y acciones). Así mismo, el PROVEEDOR debe disponer de un procedimiento de exportación controlada para auditoría o uso probatorio, cuando sea requerido por la ENTIDAD.

S7.4. Responsabilidad de almacenamiento durante la ejecución contractual

Durante la ejecución del contrato, el almacenamiento de los logs y la infraestructura necesaria para su conservación, consulta y gestión son de responsabilidad exclusiva del PROVEEDOR, sin perjuicio de los accesos y controles que defina la ENTIDAD.

S7.5. Entrega y reversibilidad al finalizar el contrato

S7.5.1. Una vez finalizado el contrato, el PROVEEDOR debe entregar a la Fiscalía General de la Nación la totalidad de los logs correspondientes al periodo contractual y a las retenciones exigidas, en el almacenamiento dispuesto por la ENTIDAD, previa coordinación técnica para la validación de capacidad y disponibilidad. La entrega debe realizarse en formatos abiertos y documentados, garantizando legibilidad e integridad de la información.

S7.5.2. El PROVEEDOR debe entregar una herramienta Open Source o con licenciamiento vitalicio (sin costes recurrentes) que permita la lectura, consulta y búsqueda de la información entregada, junto con la documentación necesaria para su instalación y uso, evitando dependencia tecnológica del PROVEEDOR o del fabricante para acceder a los registros.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S7.6. Los logs deben almacenarse bajo mecanismos de inmutabilidad que impidan su modificación o eliminación no autorizada durante el período de retención definido

S7.7. La solución puede implementarse en infraestructura en nube, híbrida o en sitio, sin restricción geográfica específica, siempre que el PROVEEDOR garantice el cumplimiento de la normativa colombiana de protección de datos personales (Ley 1581 de 2012), los principios de soberanía del dato y los requerimientos de confidencialidad, integridad, disponibilidad y trazabilidad. En caso de almacenamiento o procesamiento fuera del territorio nacional, el PROVEEDOR debe asegurar mecanismos equivalentes de protección y control definidos por la ENTIDAD.

S7.8. Pruebas de aceptación

Como condición de aceptación (por fases), el PROVEEDOR debe ejecutar y documentar pruebas que evidencien el cumplimiento de los numerales S7.1 a S7.6, consolidando los resultados en un acta y un dossier de evidencias con trazabilidad por criterio.

S7.8.1. Criterios de aceptación — S7.1 (Almacenamiento y acceso)

a) Acceso efectivo de la ENTIDAD: Evidencia de habilitación de usuarios/roles de consulta para la ENTIDAD y acceso exitoso a la plataforma/visor de logs.
b) Consulta y búsqueda: Evidencia de ejecución de búsquedas/consultas sobre logs generados por servicios del alcance, con resultados visibles.
c) Exportación: Evidencia de exportación de logs desde el visor/herramienta a un formato entregable, con archivo exportado y verificación de consistencia básica.

S7.8.2. Criterios de aceptación — S7.2 (Retención 36 meses + 36 meses cold/archive)

a) Políticas de retención configuradas: Evidencia de configuración de retención para analítica/consulta ≥ 36 meses y retención histórica ≥ 36 meses adicionales en modo cold/archive. b) Consulta/recuperación bajo requerimiento: Evidencia de ejecución de un caso de prueba de consulta o recuperación desde la retención histórica, conforme procedimiento del PROVEEDOR.

S7.8.3. Criterios de aceptación — S7.3 (Integridad, custodia y exportación controlada)

a) Controles de integridad/custodia habilitados: Evidencia de controles implementados para prevenir modificación/borrado no autorizado (inmutabilidad/WORM o equivalentes) y auditoría asociada.
b) Procedimiento de exportación controlada: Evidencia documental del procedimiento y ejecución de un caso de exportación controlada con trazabilidad (quién/qué/cuándo), para auditoría o uso probatorio.

S7.8.4. Criterios de aceptación — S7.4 (Responsabilidad del almacenamiento en ejecución)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		a) Evidencia de operación bajo responsabilidad del PROVEEDOR: Evidencia documental/técnica que soporte que el repositorio de logs, su conservación y su operación durante la vigencia contractual están a cargo del PROVEEDOR. S7.8.5. Criterios de aceptación — S7.5 (Entrega y reversibilidad / salida) a) Prueba de entrega (simulación controlada): Evidencia de una entrega de muestra representativa de logs al almacenamiento dispuesto por la ENTIDAD, con verificación de integridad/legibilidad. b) Lectura con herramienta entregada: Evidencia de lectura/consulta/búsqueda de los archivos entregados usando la herramienta Open Source o con licenciamiento vitalicio suministrada. c) Acta y dossier de evidencias: Acta de aceptación (por fase o final) y dossier de evidencias con trazabilidad a cada criterio S7.8.x.
	S8.	Servicio de Data Loss Prevention — DLP (On-premise y Nube) S8.1. Objeto S8.1.1. El PROVEEDOR debe suministrar, implementar, operar y mantener un servicio administrado de Prevención de Pérdida de Datos (DLP) para la Fiscalía General de la Nación, que permita identificar, clasificar, monitorear, prevenir y responder ante riesgos de fuga o exposición de información en ambientes On-premise, nube y/o híbridos, cubriendo como mínimo los canales: endpoint, correo/colaboración suite (M365), web/SSE (SWG/CASB), repositorios en reposo On-premise y cloud, y controles de compartición/permisionamiento en nube/SaaS según aplique. S8.1.2. En caso de cambio de plataforma de correo, el PROVEEDOR debe aplicar el servicio sobre la nueva plataforma de correo bajo las mismas condiciones. S8.1.3. El servicio de DLP debe integrarse con los demás módulos de DLP asociados a los demás servicios, incluidos en esta ficha técnica. S8.1.4. La ENTIDAD podrá definir y suministrar al inicio del contrato un esquema de clasificación de la información (por niveles de sensibilidad o criticidad), el cual debe ser adoptado por el PROVEEDOR para la gestión de logs, eventos, evidencias y demás datos tratados en el servicio. En ausencia de dicha clasificación formal, el PROVEEDOR deberá aplicar controles equivalentes que garanticen el tratamiento de la información conforme a su nivel de sensibilidad, en alineación con las políticas de seguridad de la ENTIDAD y la normativa vigente. S8.1.5. El servicio DLP debe estar integrado con el SOC como servicio 24x7 para correlación (SIEM), automatización (SOAR), gestión ITIL estricta (ITSM como system of record), enriquecimiento por CMDB y con la herramienta de observabilidad de la ENTIDAD. S8.2. Alcance y cobertura mínima S8.2.1. Modalidad del servicio y operación

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S8.2.1.1. El DLP se prestará como servicio administrado que incluye: diseño, implementación por fases, operación, monitoreo, investigación, afinamiento de políticas, soporte a despliegue masivo, y mejora continua.

S8.2.1.2. Operación mínima: 8x5 para administración y soporte funcional; operación del servicio y escalamiento y gestión de incidentes 24x7 coordinado con el SOC (S1—S4). En caso de incidentes, donde la supervisión requiera al personal de administración y soporte, en horario adicional, el PROVEEDOR lo suministrará de acuerdo con el requerimiento.

S8.2.2. Cobertura mínima

La solución debe licenciarse para soportar, como mínimo, treinta mil (30.000) usuarios en los canales de correo electrónico, colaboración y web/SSE (SWG/CASB), y veintiséis mil (26.000) endpoints con agente de DLP de endpoint, conforme a la línea base institucional. El descubrimiento y la clasificación de datos en reposo aplican sobre los repositorios on-premise y en nube definidos por la ENTIDAD y no se limitan por número de usuarios.

S8.2.2.1. Endpoint DLP:

Capacidad de monitorear y prevenir exfiltración/uso indebido por acciones, como mínimo:

- Copia/pega, impresión, portapapeles, capturas de pantalla (cuando aplique por SO/tecnología), transferencia a USB/medios removibles, sincronización/drive, subida a web, aplicaciones de mensajería/transferencia, y uso de apps no autorizadas (cuando aplique por servicio).

- Acciones: bloquear, permitir con registro, coaching al usuario, justificación/override controlado, cuarentena y alerta.

S8.2.2.2. Correo y colaboración — M365 desde el día 1:

Inspección y control de contenido en:

- Correo saliente (y el alcance interno según defina la ENTIDAD),
- Colaboración/archivos asociados (según capacidades de M365).
- Acciones: bloquear, cuarentena, cifrar/proteger, advertir, justificación, alertar SOC.

S8.2.2.3. Web/SSE — SWG/CASB desde el día 1:

Control de carga/descarga y uso de SaaS mediante SSE (SWG/CASB), con políticas por:

- Identidad/grupo, postura, aplicación/SaaS, destino, clasificación y riesgo.
- Acciones: bloqueo, inspección, redacción, coaching y alertas.

S8.2.2.4. Datos en reposo (Discovery/Scanning) on-premise y cloud:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

La solución deberá proporcionar capacidades de descubrimiento, análisis y clasificación de información sensible almacenada en repositorios cloud/SaaS y on-premise, incluidos recursos compartidos de archivos y repositorios documentales definidos por la ENTIDAD, con reporte de:

- Ubicación, tipo de dato sensible, volumen, propietario, permisos/exposición, criticidad CMDB y priorización por riesgo.

Para los repositorios on-premise, la capacidad podrá implementarse mediante agentes en servidores, conectores SMB/NFS, nodos de escaneo independientes, APIs, plataformas de clasificación, escaneo programado o mecanismos funcionalmente equivalentes. No se exigirá la instalación obligatoria de motores directamente sobre los dispositivos de almacenamiento.

El escaneo deberá admitir ejecución programada, incremental y bajo demanda, con controles de carga, ventanas de ejecución, priorización y monitoreo de desempeño que eviten impactos significativos sobre la operación.

Los controles sobre datos en uso y en movimiento complementarán el descubrimiento de información en reposo, pero no lo sustituirán.

Nota: El descubrimiento y clasificación de datos en reposo podrá acreditarse mediante la plataforma DLP ofertada, componentes especializados o las capacidades institucionales de Microsoft Purview administradas en el numeral S23, siempre que se integren al servicio DLP y al SOC. Cuando se utilicen las capacidades de Purview de la ENTIDAD, no se exigirá al OFERENTE licenciamiento adicional de dicha plataforma ni un motor adicional de escaneo. El alcance comprende los repositorios bajo administración de la ENTIDAD (servidores de archivos, NAS, servidores y repositorios cloud/SaaS) y no incluye el escaneo de los discos locales de las estaciones de trabajo, cuya información se protege mediante los controles DLP de endpoint sobre datos en uso y en movimiento. El descubrimiento en recursos compartidos on-premise se ejecutará en ventanas programadas y con mecanismos que eviten la degradación del almacenamiento.
El enriquecimiento de los eventos y hallazgos DLP con información de la CMDB institucional podrá realizarse en la solución DLP o en los componentes SOAR/SIEM integrados al servicio, mediante API, webhooks, middleware o intercambio estructurado, siempre que la priorización por riesgo quede disponible en el SOC y en los reportes del S8.2.2.4.

S8.2.2.5. Controles en nube/IaaS:

Capacidad de detectar y soportar remediación ante:

- Compartición indebida, permisos excesivos, enlaces públicos, exposición de repositorios, configuración insegura de almacenamiento, según tecnologías definidas por la ENTIDAD. Los controles de configuración segura y postura de nube podrán satisfacerse mediante capacidades propias de la solución ofertada o mediante integración con herramientas

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

especializadas o nativas del proveedor de nube; los controles de exposición de datos en aplicaciones SaaS se mantienen como obligatorios.

S8.3. Despliegue por fases: Piloto + OLAs

S8.3.1. M1 — Alistamiento y prerrequisitos

S8.3.1.1. El PROVEEDOR debe ejecutar alistamiento que incluya:

- Arquitectura objetivo (on□premise/nube/híbrida) y controles de seguridad (RBAC/MFA, cifrado, segregación).
- Plan de despliegue endpoint DLP (distribución, compatibilidad, rendimiento, coexistencia con EDR).
- Integración M365 (mecanismos soportados) y SSE desde el día 1.
- Integraciones SOC: SIEM/SOAR/ITSM/CMDB.
- Taxonomía de datos sensibles y priorización por servicios críticos.

S8.3.2. Fase 1 — Piloto (≈ 5.000 endpoints)

S8.3.2.1. El piloto debe cubrir ~5.000 endpoints y obligatoriamente:

- Endpoint DLP en esos endpoints,
- DLP para M365 correo/colaboración desde el día 1,
- DLP en SSE (SWG/CASB) desde el día 1,
- Discovery en al menos 1 repositorio on-premise y 1 repositorio cloud/SaaS definidos por la ENTIDAD.

S8.3.2.2. El piloto se considera exitoso con los criterios de aceptación (S8.12) y con umbrales de estabilidad/rendimiento definidos (ver S8.8).

S8.3.3. Fase 2 — Despliegue por OLAs (toda la ENTIDAD)

S8.3.3.1. El despliegue restante se realizará por OLAs con cronograma propuesto y aprobado, incluyendo:

- Ventanas de cambio, plan de reversión, comunicación a usuarios y “hypercare”.
- Gestión de excepciones con vencimiento y aprobación.

S8.4. Clasificación y detección de datos sensibles (base de políticas)

S8.4.1. Modelo de clasificación

S8.4.1.1. El PROVEEDOR debe soportar el esquema de clasificación vigente de la ENTIDAD o proponer uno compatible, y mapearlo a políticas DLP por servicio.

S8.4.2. Técnicas mínimas de detección

S8.4.2.1. El DLP debe soportar como mínimo:

- Reglas por patrones (regex), diccionarios/keywords y validación contextual.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Exact Data Match / fingerprinting o técnica equivalente verificable para datos estructurados/no estructurados.
- Clasificación/etiquetado por metadatos y contexto (aplicación, destino, dominio, usuario, grupo, CI/CMDB, índice de clasificación).

S8.4.2.2. Versionado y auditoría de políticas (quién/qué/cuándo) y capacidad de afinamiento sin caída del servicio.

S8.4.3. Catálogo inicial y mejora continua

S8.4.3.1. Catálogo inicial mínimo: Se debe implementar, cómo mínimo 25 políticas/casos de uso DLP (distribuidos por servicio: endpoint, M365, SSE y discovery).

S8.4.3.2. Mejora continua: implementar nuevas políticas/casos de uso por mes, priorizadas con la ENTIDAD, con evidencia de puesta en producción y medición de falsos positivos, aplicando el proceso de gestión de cambio establecido por la ENTIDAD.

S8.5. Integraciones (M365 + SSE desde día 1) y cloud

S8.5.1. M365 (desde el día 1)

S8.5.1.1. Para Microsoft 365/Entra, la integración y recolección/acción debe realizarse mediante mecanismos soportados por la plataforma (Microsoft Graph / Office 365 Management Activity API u otros soportados), evitando métodos no aplicables.

S8.5.2. SSE (SWG/CASB) (desde el día 1)

S8.5.2.1. Integración con SSE para aplicar políticas DLP en tráfico web/SaaS, con trazabilidad de decisiones (bloqueo/permitido/sobreescritura) y evidencia exportable.

S8.5.2.2. La solución deberá proporcionar visibilidad y control sobre el uso de aplicaciones y servicios de inteligencia artificial utilizados por los usuarios de la ENTIDAD, incluyendo capacidades para descubrir aplicaciones de IA generativa, aplicar controles DLP sobre información enviada a dichos servicios, identificar aplicaciones no autorizadas y generar eventos para integración con SOC, SIEM y DLP.

S8.5.3. Nube/IaaS y repositorios cloud

S8.5.3.1. Soporte de discovery y controles de exposición/compartición en repositorios cloud/SaaS definidos por la ENTIDAD, mediante APIs y logs soportados.

S8.6. Integración con SOC/SIEM/SOAR/ITSM/CMDB y Observabilidad

S8.6.1. SIEM / SOC como servicio

S8.6.1.1. Envío de eventos/alertas al SIEM del SOC como servicio con campos mínimos: usuario, dispositivo, canal, política,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		acción, clasificación/etiqueta, destino, marca de tiempo, evidencia (con enmascaramiento si aplica), CI/servicio. S8.6.2. SOAR / SOC como servicio S8.6.2.1. Disparadores para playbooks: cuarentena, bloqueo de envío, revocación de compartición, bloqueo en SSE, solicitud de re-etiquetado, etc. S8.6.2.2. Acciones disruptivas con human-in-the-loop salvo escenarios preaprobados. S8.6.3. ITSM institucional (system of record) S8.6.3.1. Todo incidente/caso DLP definido por la ENTIDAD debe generar ticket automático en ITSM con: • Severidad/prioridad, CI/CMDB, evidencia, acciones ejecutadas/recomendadas, timeline. S8.6.3.2. Integración con idempotencia, colas/reintentos y trazabilidad de transacciones (éxito/fallo/latencia). S8.6.4. CMDB S8.6.4.1. Enriquecimiento con criticidad/propietario/servicio y priorización automática. S8.7. Acciones de política y gobierno (prevenir + educar + controlar) S8.7.1. Acciones mínimas por servicio: bloquear, permitir con registro, cuarentena, cifrado/protección (si aplica), entrenamiento, sobreescritura con justificación, alertar al SOC. S8.7.2. La acción 'cifrado/protección' del S8.7.1 podrá ejecutarse mediante acciones de protección equivalentes: cifrado nativo, cifrado provisto por un componente integrado al DLP, aplicación de etiquetas con protección de Microsoft Purview de la ENTIDAD (S23) o cifrado del canal (correo o medio removible), conforme a la política aprobada y con alertamiento al SOC. S8.7.3. Excepciones: deben ser aprobadas, registradas en ITSM, con fecha de expiración, y auditables. S8.8. Capacidad, desempeño y escalabilidad (verificable y por tramos) S8.8.1. Requisitos mínimos para piloto de 5.000 endpoints S8.8.1.1. El servicio debe demostrar capacidad de operación estable para ~5.000 endpoints en piloto, sin degradar de forma material el desempeño del endpoint (CPU/RAM/IO) por encima de umbrales razonables definidos en el plan de despliegue. S8.8.1.2. El PROVEEDOR debe entregar un plan de despliegue masivo con:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Estrategia de lanzamiento (anillos/canales), control de versiones, restablecimiento,
- Compatibilidad OS, coexistencia con EDR y otras herramientas,
- Ventanas y “hypercare”.

S8.8.2. Dimensionamiento por servicio y expansión por tramos

S8.8.2.1. El OFERENTE debe presentar dimensionamiento por servicio (endpoint, M365, SSE, descubrimiento), con supuestos y márgenes de crecimiento.

S8.8.2.2. Escalabilidad por tramos verificables: # endpoints, volumen de correo/eventos API, capacidad descubrimiento, conectores SaaS, retención 36 meses (sin cláusulas “ilimitadas” o “sin costo adicional” ambiguas).

S8.9. Retención, integridad y custodia

S8.9.1. Retención mínima: 36 meses consultables y exportables de:

- Eventos/alertas/casos DLP, bitácoras, cambios de políticas, reportes, evidencias asociadas.

S8.9.2. Integridad y protección contra borrado/modificación no autorizada: preferible inmutabilidad/WORM o controles equivalentes verificables (hashing, segregación de funciones, auditoría).

S8.10. Privacidad, minimización de contenido y seguridad del servicio

S8.10.1. El servicio DLP debe implementar minimización de exposición de contenido, accesos restringidos y auditoría completa.

S8.10.2. Controles: MFA, RBAC, segregación de funciones, cifrado en tránsito y reposo, y separación lógica de datos (tenant/espacio segregado).

S8.10.3. Disponibilidad: el servicio debe cumplir la disponibilidad establecida en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

S8.11. SLAs, KPIs y reportes

S8.11.1. SLAs por severidad alineados al SOC (medición oficial desde ITSM).

S8.11.2. Reporte mensual mínimo:

- Volumen por servicio, alertas→casos→incidentes,
- Falsos positivos/negativos estimados y afinamiento realizado,
- Top políticas disparadas y tendencias por servicio crítico (CMDB),
- Salud de integraciones (M365, SSE, SIEM, ITSM, CMDB) y colas,
- MTTD/MTTR y cumplimiento de SLA.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S8.11.3. Reporte por incidente y ad hoc: timeline, impacto, evidencia, acciones, restore/verificación si aplica, RCA y lecciones aprendidas.

S8.12. Pruebas de aceptación

S8.12.1. Aceptación del piloto (≈ 5.000 endpoints)

El PROVEEDOR debe evidenciar:

1. Endpoint DLP (5.000 endpoints):
   a. Política de control USB (bloqueo/alerta) para documento sensible.
   b. Generación de evento SIEM y ticket ITSM con evidencia.
2. M365 DLP (día 1):
   a. Detección y acción (cifrar/cuarentena/bloquear) ante envío de dato sensible a dominio externo.
   b. Evidencia completa y trazabilidad en ITSM.
3. SSE DLP (día 1):
   a. Bloqueo/alerta ante subida de dato sensible a SaaS no autorizado o canal definido.
   b. Evidencia de identidad/usuario y decisión de política.
4. Discovery (reposo):
   a. Escaneo de 1 repositorio on-premise + 1 repositorio cloud/SaaS con hallazgos priorizados.
   b. Generación de tareas/ITSM para remediación (permisos, re etiquetado, corrección de exposición).
5. Integración SOC/ITSM/CMDB end to end:
   a. Ticket automático con CI vinculado a CMDB y priorización por criticidad.
   b. Actualización del ticket con evidencias y acciones.

S8.12.2. Aceptación por OLAs (despliegue)

Para cada OLA, se validará:

- Políticas por canal activas,
- Estabilidad del agente endpoint y plan de rollback probado,
- Métricas de adopción (endpoints protegidos vs plan) y reporte de incidentes.

S8.13. Documentación técnica exigida.

El PROVEEDOR debe anexar:

- Arquitectura (on prem/nube/híbrida) por servicio
- Dimensionamiento por servicio y retención 36 meses,
- Plan de despliegue masivo (piloto 5.000 endpoints + OLAs), rollback/hypercare,
- Matriz de integraciones: M365 (día 1), SSE (día 1), SIEM/SOAR/ITSM/CMDB, Observabilidad, repositorios.
- Matriz de cumplimiento con evidencia (página/párrafo de fichas técnicas)
- Runbooks operativos, gobierno de excepciones/overrides y plan de salida.

S8.14. Plan de salida

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		Exportación completa de políticas, configuraciones, excepciones, inventarios discovery, eventos/alertas/casos/evidencias y reportes (36 meses), y documentación/runbooks para transición. Seguir el plan de transición establecido en el Anexo Técnico 7 — Protocolo de Transición.
	S9.	Servicio de Centro de Operaciones de Seguridad — SOC S9.1. Objeto S9.1.1. El PROVEEDOR debe prestar el servicio de un Centro de Operaciones de Seguridad (SOC) 24x7 que incluya, como mínimo: recolección, normalización, correlación, detección, investigación, priorización y gestión de incidentes y respuesta/contención activa ante eventos de ciberseguridad para la Fiscalía General de la Nación, en ambientes on-premise, nube y/o híbridos, como mínimo 1.500 activos definidos por la ENTIDAD. S9.2. Alcance y cobertura mínima S9.2.1. Cobertura operacional S9.2.1.1. El servicio de SOC debe operar 24x7, incluyendo festivos, con turnos y recursos suficientes para atender la demanda del servicio. S9.2.1.2. El servicio debe incluir, como mínimo, niveles de atención L1/L2/L3 o equivalentes, con reglas de escalamiento y contacto designado por la ENTIDAD. S9.2.1.3. El modelo de operación del SOC corresponde a un esquema de SOC como servicio (tercerizado), en el cual el PROVEEDOR es responsable de la operación técnica integral (monitoreo, correlación, respuesta y gestión de logs), manteniendo integración con las plataformas institucionales de la ENTIDAD (ITSM y Observabilidad), y garantizando acceso, visibilidad y control por parte de la ENTIDAD, sin que ello implique un modelo de operación híbrido. S9.2.1.4. El PROVEEDOR debe incorporar mecanismos de escalabilidad que permitan el crecimiento progresivo del entorno durante la vigencia del contrato, sin afectación del servicio, incluyendo expansión de capacidad de ingestión (EPS), almacenamiento, retención y conectores. S9.2.2. Cobertura de activos y entornos S9.2.2.1. La ENTIDAD definirá el universo inicial de activos (mínimo 1.500) y su criticidad (vía CMDB). S9.2.2.2. Se debe cubrir infraestructura on-premise y nube (incluyendo Azure y otros proveedores definidos por la ENTIDAD). S9.2.2.3. Las soluciones SIEM y SOAR del SOC como servicio deben soportar, de manera nativa o mediante conectores, la

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

integración de fuentes heterogéneas sin dependencia de marca específica, formulando el cumplimiento por capacidades funcionales.

S9.3. Fuentes mínimas priorizadas

El PROVEEDOR debe integrar y mantener, como mínimo, las siguientes fuentes críticas priorizadas, sin perjuicio de incorporar otras fuentes definidas por la ENTIDAD:

1. EDR/XDR (telemetría, alertas, acciones de respuesta).
2. Directorio Activo on□premise y Microsoft Entra ID (autenticaciones, auditoría, cambios).
3. Correo y seguridad asociada (Microsoft 365 u otras plataformas).
4. Firewall perimetral.
5. WAF.
6. Proxy/SSE.
7. DLP.
8. VPN/ZTNA.
9. Motores de bases de datos (SQL Server, Oracle, MySQL u otros definidos).
10. Infraestructura crítica adicional (servidores, hipervisores, aplicaciones críticas, switches, SD WAN y demás dispositivos que hagan parte del servicio de seguridad, etc.).

Nota de integración Cloud

- □ Para Microsoft 365/Entra, la recolección debe realizarse mediante mecanismos soportados por la plataforma Office 365 Management Activity API y/o Microsoft Graph según aplique, y no mediante WMI.

- □ Para Azure, la recolección de logs/metricas debe soportar el uso de Diagnostic settings (Azure Monitor) hacia destinos compatibles (Event Hub, Storage, Log Analytics u otros), según arquitectura definida por la FGN.

S9.4. Capacidad, ingestión y desempeño (EPS, latencia y escalabilidad)

S9.4.1. Capacidad mínima

S9.4.1.1. El servicio debe soportar el monitoreo de mínimo 1.500 activos.

S9.4.1.2. La capacidad de ingestión debe dimensionarse con base en eventos por segundo (EPS). Para evitar ambigüedades, se establece:

- □ EPS sostenidos mínimos: 10.000 EPS.
- □ EPS pico mínimo: 30.000 EPS (equivalente a 20 EPS por activo para 1.500 activos), o el valor que resulte del dimensionamiento real acordado en el plan de implementación.

S9.4.1.3. El servicio SOC debe soportar una capacidad mínima de ingestión de 10.000 EPS sostenidos y 30.000 EPS en picos. Estos valores corresponden al dimensionamiento base inicial y deben ser ampliados por el PROVEEDOR conforme al crecimiento del entorno,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

garantizando escalabilidad sin interrupciones del servicio, mediante mecanismos de expansión progresiva en ingestión, almacenamiento y procesamiento durante la vigencia del contrato.

S9.4.2. Latencia de detección

S9.4.2.1. El servicio debe generar alertas con latencia máxima por severidad establecida en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio, contada desde la recepción del evento hasta la generación del caso/incidente.

S9.4.3. Escalabilidad

S9.4.3.1. La solución SIEM del SOC como servicio debe permitir escalabilidad de componentes (ingestión, búsqueda, almacenamiento) sin interrupción del servicio.

S9.4.3.2. La escalabilidad debe ofrecerse mediante modelo de expansión por tramos (EPS, retención, almacenamiento, conectores), de forma transparente y verificable.

S9.5. Recolección, normalización y métodos de integración

S9.5.1. Métodos de recolección

S9.5.1.1. La solución debe recolectar logs/eventos usando métodos estándar, incluyendo, como mínimo, los siguientes cuando aplique:

- Syslog, SNMP, WMI (solo para fuentes Windows on-prem), APIs/REST, agentes, JDBC, LDAP, SSH, y protocolos TCP/UDP genéricos seguros; así como integraciones específicas para flujos (NetFlow/sFlow/IPFIX) si la ENTIDAD lo requiere.

S9.5.2. Normalización y extensibilidad

S9.5.2.1. El PROVEEDOR debe disponer de normalizadores para múltiples marcas y tecnologías.

S9.5.2.2. Debe permitir ajuste de estructuras de datos a ingestar sin interrumpir la ingestión ni provocar caída del servicio; los cambios deben quedar auditados.

S9.5.3. Correlación cruzada

S9.5.3.1. El servicio debe realizar correlación cruzada entre múltiples fuentes (firewalls, EDR/XDR, directorios, correo, WAF, proxy/SSE, DLP, VPN/ZTNA, bases de datos, servidores, etc.), produciendo alertas enriquecidas y priorizadas.

S9.6. Analítica avanzada (IA/ML/UEBA) y “detección proactiva”

S9.6.1. La solución debe incluir capacidades de analítica avanzada para mejorar priorización y reducir falsos positivos.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S9.6.2. El PROVEEDOR debe entregar un catálogo inicial de casos de uso (a definir junto con la ENTIDAD en la etapa de alistamiento) y un plan de mejora continua (nuevos casos de uso por mes).

S9.6.3. Las alertas deben ser explicables mediante evidencia (fuentes, campos, regla/caso de uso, contexto CMDB) y trazables en ITSM.

S9.6.4. Analítica avanzada y comportamiento de usuarios y entidades. La plataforma SIEM/SOC deberá proporcionar capacidades de analítica avanzada y análisis de comportamiento de usuarios y entidades, mediante mecanismos nativos, módulos integrados o capacidades funcionalmente equivalentes, con el propósito de construir líneas base de comportamiento, detectar desviaciones y actividades anómalas, generar niveles de riesgo, priorizar alertas, reducir falsos positivos y apoyar la identificación de amenazas internas, cuentas comprometidas, abuso de privilegios y accesos no habituales.

La solución deberá correlacionar señales de identidad, endpoint, correo electrónico, red, VPN/ZTNA, aplicaciones, servicios cloud, accesos privilegiados e inteligencia de amenazas, incorporando contexto de CMDB y criticidad del activo.

Las alertas deberán ser explicables y trazables, incluyendo evidencia, fuentes, campos, línea de tiempo y factores de riesgo utilizados. El cumplimiento podrá demostrarse mediante documentación técnica oficial, demostración funcional o pruebas de aceptación acordadas con la ENTIDAD.

La totalidad de los componentes y licencias requeridos para proporcionar esta capacidad deberá quedar incluida dentro del servicio SIEM/SOC.

S9.7. Almacenamiento, retención y custodia: 36 meses consultables (hot/warm) y 36 meses adicionales en modalidad cold/archive.

S9.7.1. Retención operativa (Hot/Warm)

S9.7.1.1. La solución debe conservar y permitir búsqueda/correlación de logs por un período mínimo de 36 meses en modo consultable (hot/warm).

S9.7.2. Retención adicional (Cold/Archive)

S9.7.2.1. Cada registro deberá conservarse durante un periodo mínimo de treinta y seis (36) meses en modo consultable hot/warm y treinta y seis (36) meses adicionales en modalidad cold/archive, para una retención total de setenta y dos (72) meses. Durante la vigencia contractual, la infraestructura, operación, dimensionamiento y costos de almacenamiento necesarios para cumplir esta obligación estarán a cargo del PROVEEDOR. En la modalidad cold/archive se deberá garantizar:

- disponibilidad para consulta o recuperación bajo requerimiento,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- mecanismos de integridad (verificación periódica de consistencia),
- exportación controlada para propósitos probatorios o de auditoría.

S9.7.3. Ubicación, custodia y confidencialidad

S9.7.3.1. El almacenamiento podrá ser local, nube o en el SOC, según arquitectura acordada, pero debe cumplir controles de seguridad (cifrado, acceso, segregación, registro de auditoría).

S9.7.3.2. Al finalizar el contrato, el PROVEEDOR deberá entregar a la ENTIDAD la totalidad de los logs bajo su custodia, incluidos los registros consultables y los conservados en modalidad cold/archive, en formatos abiertos y documentados, garantizando su integridad y legibilidad. Asimismo, deberá entregar una herramienta Open Source o con licenciamiento vitalicio que permita su lectura, consulta y búsqueda. A partir de la aceptación de la entrega, la custodia y conservación posterior estarán a cargo de la ENTIDAD, salvo que exista una extensión contractual expresa del servicio.

S9.7.3.3. En caso de tratamiento de datos personales, el PROVEEDOR debe cumplir normatividad aplicable en Colombia.

S9.8. Continuidad de ingestión y calidad de datos

S9.8.1. El PROVEEDOR debe implementar mecanismos de store-and-forward, buffers persistentes, reintentos y colas para minimizar pérdida ante fallas de conectividad o indisponibilidad temporal de fuentes/destinos.

S9.8.2. Se exigirá un SLO medible de entrega/ingestión, conforme a los niveles de servicio establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio, y reporte mensual de:

- eventos recibidos vs. esperados,
- brechas (“gaps”) y tiempos de recuperación,
- causas raíz y acciones correctivas.

S9.8.3. Se evitarán formulaciones absolutas (“no debe existir pérdida”) dado que incluso arquitecturas cloud de logging pueden no ofrecer garantías transaccionales completas en todos los escenarios; por tanto, se exige SLO + controles + evidencia.

S9.9. Consolas, acceso, visibilidad y reportes

S9.9.1. Acceso concurrente y visor

S9.9.1.1. La ENTIDAD debe contar con acceso de consulta a visor de eventos/logs y tableros, con concurrencia mínima de 10 usuarios.

S9.9.1.2. Se deben implementar roles y segregación de funciones (consulta, analista, administrador) y auditoría de actividades.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S9.9.2. Dashboards y reportes configurables

S9.9.2.1. El servicio debe proveer una consola tipo dashboard con gráficos/tablas configurables y vistas por: severidad, activo/CI, servicio CMDB, fuente, MITRE/kill chain (si aplica), tendencias y KPIs.

S9.9.2.2. Debe permitir reportes parametrizables (custom) y exportación.

S9.10. Gestión de incidentes, SLAs y operación SOC (24x7)

S9.10.1. Modelo de gestión de incidentes

S9.10.1.1. El servicio debe operar un proceso formal de gestión de incidentes (detección, análisis, contención, erradicación, recuperación, lecciones aprendidas), alineable a buenas prácticas de respuesta a incidentes y gestión estructurada.

S9.10.1.2. Debe existir matriz de severidades S1—S4 definida con la ENTIDAD, con criterios por impacto y criticidad del activo/servicio (CMDB).

S9.10.2. Niveles de servicio. Los tiempos de atención, notificación y contención por severidad, su método de medición y las penalidades aplicables son los definidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.
Nota: Los SLAs deben ponderarse por criticidad CMDB (activos/servicios críticos pueden escalar severidad/prioridad automáticamente).

S9.11. Integración con ITSM de la ENTIDAD

S9.11.1. El PROVEEDOR debe integrar la plataforma SIEM del SOC como servicio con la herramienta ITSM de la ENTIDAD, de modo que todo incidente y eventos correlacionados que la ENTIDAD defina genere automáticamente un ticket/caso en ITSM, incluyendo: clasificación, severidad, prioridad, asignación, evidencias y trazabilidad.

S9.11.2. La integración debe soportar, como mínimo:
- creación de tickets,
- actualización automática del ticket con estados/evidencias,
- sincronización de estados (bidireccional, cuando el ITSM lo permita),
- trazabilidad completa de transacciones (éxito/fallo/reintentos/latencia).

S9.11.3. La integración debe realizarse mediante mecanismos estándar soportados por el ITSM (APIs/servicios/webhooks o equivalentes), evitando requisitos direccionadores por marca.

S9.12. Uso de la CMDB (enriquecimiento y priorización)

S9.12.1. El PROVEEDOR debe consumir la CMDB de la ENTIDAD para enriquecer eventos/alertas con: criticidad, propietario, servicio relacionado, ambiente y metadatos del CI.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S9.12.2. Cada ticket en ITSM debe quedar vinculado al CI correspondiente en CMDB, habilitando priorización automática y reportes por servicio/proceso.

S9.12.3. El PROVEEDOR debe reportar hallazgos de inconsistencias CMDB (CI inexistente, atributos faltantes) como tickets de mejora/problema según el modelo ITSM de la ENTIDAD.

S9.13. Contención activa, automatización y gobernanza

S9.13.1. Capacidades de contención activa

S9.13.1.1. La plataforma y el servicio deben permitir ejecutar acciones de respuesta, tales como:

- bloqueo de IP/URL/dominio en firewall/WAF/proxy/SSE,
- aislamiento de endpoints (EDR),
- deshabilitación/revocación de sesiones de usuarios (AD/Entra),
- cuarentena/bloqueo de correo/remitente,
- bloqueo de hash/archivo (EDR), según integraciones disponibles y autorizaciones de la ENTIDAD.

S9.13.2. Gobernanza obligatoria

S9.13.2.1. El PROVEEDOR debe implementar playbooks/runbooks de respuesta, con dos modalidades:

- Automática: solo para escenarios preaprobados por la ENTIDAD.
- Con aprobación: para acciones de alto impacto, registrando aprobación en ITSM (quién/cuándo/qué) antes de ejecutar.

S9.13.2.2. Toda acción ejecutada debe quedar registrada con evidencia en el ticket ITSM y en bitácoras del SOC.

S9.14. Inteligencia de amenazas y enriquecimiento

S9.14.1. El servicio debe permitir integración con fuentes de inteligencia de amenazas (IoCs: dominios, IPs, URLs, hashes) mediante APIs o mecanismos equivalentes, y enriquecer casos con reputación/contexto.

S9.14.2. El PROVEEDOR debe documentar fuentes, periodicidad de actualización y evidencia de uso en casos.

S9.15. Seguridad de la plataforma y controles de acceso

S9.15.1. Acceso administrativo y de analistas con MFA, roles, segregación y trazabilidad.

S9.15.2. Cifrado en tránsito (TLS) y en reposo; registro de actividades administrativas y accesos.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S9.15.3. Separación lógica de datos de la ENTIDAD (tenant/espacio dedicado o segregación equivalente), evitando exposición a terceros. S9.16. Entregables y reportes El PROVEEDOR debe entregar como mínimo: • Informe semanal de incidentes de seguridad detectados (resumen ejecutivo + detalle técnico). • Informe mensual de incidentes priorizados por servicios críticos (CMDB), con KPIs (MTTD, MTTR, volumen, tendencias, top casos de uso, afinamiento y falsos positivos) y plan de mejora. • Informe mensual de actividades realizadas para optimización del monitoreo (onboarding, conectores, ajustes de correlación, mejoras). • Evidencia de cumplimiento de SLAs (por severidad) y de SLO de ingestión (calidad de datos). S9.17. Pruebas de aceptación Como condición de aceptación del servicio (puesta en marcha y/o por fases), el PROVEEDOR debe ejecutar y documentar pruebas que evidencien: • Onboarding de las Top 10 fuentes priorizadas (S9.3) y correlación básica multi-fuente. • Integración ITSM: creación automática de tickets para eventos de prueba S1—S4, con campos mínimos y evidencias. • Vinculación CMDB: tickets enlazados a CI correcto y priorización por criticidad. • Contención activa: ejecución controlada de al menos 3 playbooks (bloqueo IP, aislamiento endpoint, acción sobre identidad) con trazabilidad completa en ITSM (aprobación cuando aplique). • Retención: evidencia de configuración para 36 meses hot/warm y 3 años cold/archive, con procedimiento de recuperación/exportación. • Continuidad de ingestión: simulación de caída de enlace y verificación de buffer/reintentos y reporte de gaps (S9.8). S9.18. Documentación técnica exigida. El PROVEEDOR debera entregar al inicio de la ejecución del contrato: • Datasheets/fichas técnicas de las plataformas ofertadas, indicando hoja y párrafo donde se evidencie el cumplimiento. • Descripción de arquitectura propuesta (on-prem/nube/híbrida), dimensionamiento EPS/retención y controles de seguridad. • Alcance de integraciones (ITSM, CMDB, EDR, M365/Entra, Azure, firewalls, etc.) y plan de onboarding. • Propuesta de SLAs/KPIs y modelo de gobernanza de playbooks.
	S10.	Plataforma SIEM (como parte del servicio SOC 24x7)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S10.1. Alcance del componente SIEM

S10.1.1. La ENTIDAD requiere que el SOC como servicio (S9) se soporte en una plataforma SIEM que habilite, como mínimo, las capacidades funcionales, técnicas, operativas, de aseguramiento, trazabilidad y administración descritas en el presente numeral, además de las exigencias aplicables al servicio SOC definidas en el numeral S9 y demás documentos del proceso.

S10.2. SIEM dedicado y exclusivo para la ENTIDAD

S10.2.1. Dedicación y Exclusividad.

La plataforma SIEM ofrecida para la prestación del servicio debe operar de manera dedicada y exclusiva para la Fiscalía General de la Nación, de tal forma que su operación, configuración, almacenamiento lógico, contenido de detección, bitácoras administrativas y recursos asociados correspondan únicamente a la ENTIDAD durante toda la vigencia del contrato.

S10.2.2. Aislamiento verificable.

El OFERENTE debe describir y demostrar en su arquitectura propuesta el mecanismo de dedicación y aislamiento del SIEM para la ENTIDAD, ya sea mediante tenant/espacio dedicado, instancia dedicada, espacio lógico exclusivo o mecanismo equivalente de segregación verificable.
La demostración debe soportarse con evidencia documental del fabricante y/o mediante pruebas de aceptación, de forma que se acredite que no existe exposición, mezcla o acceso no autorizado por parte de terceros.

S10.3. Integración con la herramienta de Observabilidad de la ENTIDAD

S10.3.1. Integración SIEM—Observabilidad.

El SIEM debe integrarse con la herramienta de Observabilidad de la ENTIDAD, mediante mecanismos estándar soportados por las plataformas (APIs, conectores, servicios de integración o equivalentes), permitiendo el intercambio de información y visibilidad operacional que la ENTIDAD defina (envío/consulta de eventos relevantes, métricas operativas de la plataforma SIEM y estado de pipelines).

S10.3.2. Alcance mínimo de la integración.

La integración debe permitir, como mínimo:
a) Publicación desde el SIEM hacia Observabilidad de señales que la ENTIDAD determine (eventos operativos, salud de ingesta, estado de conectores, colas, caídas de conectores, fallos de procesamiento o degradaciones del servicio);
b) la trazabilidad de las transacciones de integración incluyendo como mínimo éxito, fallo, reintentos y latencia;

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

c) la disponibilidad de una bitácora consultable por la ENTIDAD sobre las transacciones e incidentes asociados a la integración.
d) la consulta o intercambio de información operacional relevante para la supervisión de la plataforma;

S10.4. Gobierno de contenido de detección (reglas, casos de uso y ciclo de vida) — específico SIEM

S10.4.1. Gestión del ciclo de vida de reglas/casos de uso. El SIEM debe permitir la administración integral del ciclo de vida de reglas, casos de uso, correlaciones, contenido analítico y elementos asociados al proceso de detección, incluyendo como mínimo: versionado, control de cambios, aprobación, despliegue controlado, y capacidad de reversión (rollback) ante fallos, conservando evidencia de quién realizó el cambio, cuándo lo realizó y qué fue modificado.

S10.4.2. Entornos de prueba.

El PROVEEDOR debe disponer de un mecanismo verificable para validar cambios de contenido del SIEM antes de aplicarlos en producción, incluyendo reglas, casos de uso, parsers, normalizadores, dashboards y configuraciones relacionadas. Se admitirá equivalencia funcional siempre que el PROVEEDOR demuestre que el mecanismo reduce el riesgo de degradación, indisponibilidad, pérdida de trazabilidad o alteración no controlada del servicio.

S10.4.3. Evidencia explicable. Para cada alerta, evento correlacionado o caso generado por el SIEM, la plataforma debe permitir registrar y consultar la evidencia que explica la detección, incluyendo como mínimo las fuentes involucradas, los campos relevantes, el contenido de detección asociado (clave y regla/caso de uso) y los elementos necesarios para su trazabilidad y validación técnica en coherencia con el requisito de alertas explicables.

S10.5. Modelo de datos y calidad de normalización (específico SIEM)

S10.5.1. Esquema normalizado consultable.

El SIEM debe soportar un esquema normalizado de eventos, con campos comunes consultables, que permita correlación, búsqueda, análisis e investigación consistentes entre tecnologías heterogéneas y múltiples fuentes de información.

S10.5.2. Gestión de parsers/normalizadores.

El SIEM debe permitir como mínimo:
a) identificar el parser o normalizador aplicado a cada evento;
b) auditar cambios realizados a parsers y normalizadores;
c) mantener compatibilidad de consultas, dashboards, reportes y correlaciones después de cambios en el tratamiento de eventos, mediante mecanismos de mapeo, alias o equivalentes que eviten la ruptura de contenido previamente implementado como reportes y correlaciones existentes.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S10.5.3. Control de “drift” de fuentes.

El PROVEEDOR debe implementar un mecanismo para detectar y gestionar cambios en formato de logs (“drift”), estructura o contenido de los registros generados por las fuentes integradas al SIEM, con el fin de identificar desviaciones o “drift” que afecten la correcta ingesta, normalización, correlación o explotación de los eventos.
La gestión de estos cambios debe tratarse como actividad controlada, con registro de evidencias, diagnóstico, ajuste aplicado y validación posterior.

S10.6. Capacidades de búsqueda, investigación y exportación técnica

S10.6.1. Búsqueda avanzada.

El SIEM debe permitir búsquedas avanzadas por campos (usuario, activo, CI/servicio, dirección origen/ dirección destino, criticidad, severidad, marcas de tiempo - timestamps) y soportar pivoteo de investigación entre eventos correlacionados.

S10.6.2. Exportación técnica.

El SIEM debe permitir exportación controlada de resultados de búsqueda, evidencias y artefactos de investigación para fines técnicos, probatorios, de auditoría o de control, bajo controles de acceso y con trazabilidad de quién exporta, qué exporta y cuándo lo exporta.

S10.6.3. Sincronización de tiempo.

El SIEM debe soportar normalización de marca temporal y evidenciar el uso de mecanismos de sincronización horaria (NTP o equivalente) para garantizar consistencia de líneas de tiempo, correlación temporal y confiabilidad de las investigaciones.

S10.7. Alta disponibilidad, respaldo y mantenibilidad del componente SIEM

S10.7.1. Alta disponibilidad (HA) del SIEM.

El OFERENTE debe presentar una arquitectura del SIEM con componentes críticos en alta disponibilidad, evitando puntos únicos de falla en ingestión, procesamiento, búsqueda, consulta, almacenamiento y componentes de administración, acorde con los niveles de continuidad requeridos para la operación del servicio SOC 24x7.

S10.7.2. Respaldo y recuperación.

El SIEM debe contar con mecanismos de respaldo y recuperación de su configuración y contenido operativo, incluyendo como mínimo parsers, normalizadores, reglas, casos de uso, integraciones, dashboards, parámetros de administración y demás componentes necesarios para la continuidad del servicio.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

El PROVEEDOR debe mantener evidencia verificable de los procedimientos de restauración y de su capacidad de recuperación.

S10.7.3. Gestión de parches y actualizaciones.

El PROVEEDOR debe definir y ejecutar un plan de actualización, mantenimiento, patching y control de versiones del SIEM, incluyendo ventanas de mantenimiento, criterios de validación, mecanismos de reversión y evidencias de ejecución, garantizando que dichas actividades no afecten materialmente la operación del SOC ni la continuidad de la detección y monitoreo.

S10.8. Accesos, auditoría y trazabilidad propia del SIEM

S10.8.1. Bitácora completa de administración SIEM.

El SIEM debe generar, conservar y permitir consultar bitácoras detalladas de actividades administrativas, cambios de configuración y acciones operativas relevantes, incluyendo como mínimo cambios sobre reglas, casos de uso, parsers, normalizadores, conectores, cuentas, perfiles, integraciones y parámetros críticos.
La ENTIDAD debe poder consultar dichas bitácoras durante la ejecución contractual, de acuerdo con los perfiles y controles de acceso definidos.

S10.8.2. Exportación de auditoría.
La auditoría administrativa y operativa del SIEM debe poder exportarse de forma controlada para fines de auditoría, inspección, control interno, investigación y verificación contractual, sin comprometer la confidencialidad, integridad o disponibilidad de la información.

S10.9. Infraestructura SIEM actualmente disponible en la ENTIDAD

S10.9.1. Plataforma SIEM actual de la ENTIDAD

La ENTIDAD cuenta actualmente con la siguiente infraestructura SIEM:
Ubicada en Bogotá:

- un (1) FortiSIEM 3600G con licenciamiento, soporte y garantía hasta el 21 de enero de 2027;
- un (1) FortiSIEM 500F con licenciamiento, soporte y garantía hasta el 21 de diciembre de 2026;
- un (1) sistema de almacenamiento IBM FlashSystem 5000 con soporte y garantía hasta el 28 de diciembre de 2026.

Ubicada en Cali:

- un (1) FortiSIEM 2000F;
- un (1) FortiSIEM 500F.
- Con licenciamiento, soporte y garantía hasta el 21 de diciembre de 2026.

Las referencias a Fortinet, FortiSIEM, IBM y FlashSystem corresponden exclusivamente a la identificación de la infraestructura actualmente disponible en la ENTIDAD y no constituyen una exigencia

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

de marca para los componentes nuevos, alternativos o de reemplazo que proponga el OFERENTE.

S10.9.2. Uso potestativo de la infraestructura existente

A discreción del PROVEEDOR, los componentes actualmente disponibles en la ENTIDAD pueden ser utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación del servicio, siempre que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso.

La decisión de utilizar o no la infraestructura existente es responsabilidad del PROVEEDOR, sin que ello releve el cumplimiento total del objeto contractual ni de los requisitos exigidos para el servicio SOC y para el componente SIEM.

S10.9.3. Mantenimiento, soporte y garantía de los componentes existentes

En caso de que el PROVEEDOR decida incorporar dentro de su arquitectura propuesta cualquiera de los componentes SIEM actualmente disponibles en la ENTIDAD, debe asumir durante toda la ejecución del contrato y sin costo adicional para la ENTIDAD, como mínimo, las siguientes obligaciones respecto de dichos componentes:
a) mantenimiento preventivo, correctivo y evolutivo que resulte aplicable;
b) soporte técnico especializado;
c) garantía y gestión de garantía frente al fabricante o canal autorizado, cuando corresponda;
d) reposición de partes, reemplazo de componentes defectuosos
e) licenciamiento, actualización, parcheo, administración, operación, revisión de estado operativo y demás actividades necesarias para asegurar su correcto funcionamiento durante toda la ejecución contractual.

S10.9.4. Validación de vigencia tecnológica y estado de soporte

El PROVEEDOR debe verificar y garantizar, previo a la puesta en marcha y durante la ejecución contractual, que los componentes utilizados dentro de la arquitectura propuesta ya sean existentes o suministrados por él, no se encuentren en estado de EOL (End of Life), EOS (End of Support) o condición equivalente que comprometa su soporte, mantenimiento, actualización, operación segura o continuidad durante la ejecución del contrato.
Dicha validación debe estar soportada documentalmente mediante evidencia del fabricante, canal autorizado o fuente oficial técnicamente verificable.

S10.9.5. Sustitución obligatoria por fin de vida

Si durante la ejecución del contrato cualquiera de los componentes incorporados a la solución entra en estado de EOL, EOS o condición

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

equivalente, o si dicho estado se determina de forma sobreviniente, el PROVEEDOR debe, sin costo adicional para la ENTIDAD, realizar su sustitución por un componente nuevo de iguales o superiores características técnicas, funcionales, de capacidad, desempeño, disponibilidad y compatibilidad, garantizando la continuidad del servicio y la no afectación material de la operación del SOC.

La sustitución debe incluir, cuando aplique, la migración, configuración, puesta en funcionamiento, pruebas, estabilización y transferencia operativa necesarias para mantener la integridad, disponibilidad y trazabilidad del servicio.

S10.9.6. Condiciones del reemplazo

Todo reemplazo de componentes deberá garantizar plena compatibilidad con la arquitectura propuesta, continuidad del servicio, integridad de la información, preservación de configuraciones, conectores, playbooks, evidencias, registros históricos y trazabilidad aplicable. El reemplazo no podrá ocasionar una interrupción injustificada del servicio ni una disminución de las capacidades exigidas por la ENTIDAD.

S10.9.7. Responsabilidad integral sobre la arquitectura propuesta

Independientemente de que el PROVEEDOR decida utilizar o no la infraestructura existente de la ENTIDAD, es de su exclusiva responsabilidad garantizar que la arquitectura propuesta cumpla con todos los requerimientos del presente proceso, incluidos los de capacidad, disponibilidad, seguridad, soporte, interoperabilidad, continuidad, retención, trazabilidad, auditabilidad y desempeño operativo.

S10.9.8. Evaluación de compatibilidad y dimensionamiento

Si el PROVEEDOR decide utilizar componentes actualmente disponibles en la ENTIDAD, debe validar y documentar su compatibilidad, dimensionamiento, capacidad útil, desempeño y vida útil remanente respecto de la arquitectura propuesta y de la carga operativa del servicio, sin que ello implique limitación o reducción del alcance requerido por la ENTIDAD.

S10.10. Transición sin afectación material

Toda incorporación, sustitución, actualización, migración o retiro de componentes del SIEM debe ejecutarse bajo procedimiento controlado, con gestión de riesgos, plan de reversión y evidencias, evitando afectación material de la operación del SOC, pérdida de eventos, pérdida de trazabilidad o indisponibilidad no autorizada.

S10.11. No utilización de la plataforma existente

Si el PROVEEDOR decide no utilizar la infraestructura SIEM existente de la ENTIDAD, ello no lo exonera del cumplimiento integral del objeto contractual ni de los niveles de servicio exigidos. En tal caso, el

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

PROVEEDOR debe suministrar, implementar, soportar y operar por su cuenta y riesgo, y sin costo adicional para la ENTIDAD, todos los componentes de hardware, software, licenciamiento, respaldo, continuidad, seguridad e integración necesarios para garantizar capacidades iguales o superiores a las definidas por la ENTIDAD.

S10.12. Condición de componentes nuevos

Todos los componentes nuevos o de reemplazo que se suministren para garantizar la prestación del servicio deberán ser originales, nuevos, no reacondicionados, no remanufacturados, estar soportados por el fabricante y cumplir con las especificaciones técnicas, funcionales, de capacidad, seguridad y compatibilidad exigidas por la ENTIDAD.

S10.13. Riesgo a cargo del PROVEEDOR

La decisión del PROVEEDOR de utilizar o no la infraestructura existente de la ENTIDAD es de su exclusiva responsabilidad y no podrá ser invocada como causa de sobrecostos, mayores tiempos de implementación, restricciones técnicas, disminución funcional, incumplimiento de niveles de servicio o solicitud de reconocimiento económico adicional.

S10.14. Requisitos documentales del OFERENTE para el componente SIEM

S10.14.1. Evidencias en oferta (SIEM). El OFERENTE debe anexar con la oferta, como mínimo:
a) Arquitectura propuesta del SIEM, indicando expresamente si utilizará o no la infraestructura actualmente disponible en la ENTIDAD;
b) Descripción de los componentes y del mecanismo de dedicación, segregación o exclusividad del SIEM para la ENTIDAD;
c) Descripción de la integración SIEM—Observabilidad y el alcance mínimo (mecanismos, datos, trazabilidad);
d) Documento de gobernanza del contenido de detección, incluyendo gestión de reglas, casos de uso, versionado, pruebas y rollback;
e) Fichas técnicas, datasheets o documentación oficial del fabricante, indicando hoja, sección o párrafo donde se evidencien las capacidades ofertadas, en línea con la exigencia documental del proceso;
f) la validación documental del estado de soporte y vigencia tecnológica de los componentes que conformarán la solución.

S10.15. Pruebas de aceptación específicas del componente SIEM

S10.15.1. Validación de dedicación.

Durante la puesta en marcha, el PROVEEDOR debe evidenciar la condición de SIEM dedicado o exclusivo para la ENTIDAD, incluyendo el mecanismo de segregación, los roles, cuentas, controles de acceso

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		y la separación de datos, configuraciones y bitácoras, dejando evidencia documental y técnica de la validación realizada. S10.15.2. Validación SIEM—Observabilidad. El PROVEEDOR debe ejecutar pruebas documentadas de integración entre el SIEM con la herramienta de Observabilidad de la ENTIDAD, acreditando el envío, recepción, consulta o intercambio de la información acordada, así como la trazabilidad de transacciones, errores, reintentos y latencias. S10.15.3. Validación de gobierno de contenido. El PROVEEDOR debe demostrar, como mínimo, el versionado de una regla o caso de uso, su despliegue controlado, la ejecución de un rollback y la generación de evidencia en bitácoras, reportes o registros de auditoría. S10.15.4. Validación de la infraestructura existente (cuando aplique). Cuando el PROVEEDOR incorpore en la arquitectura propuesta alguno de los componentes actualmente disponibles en la ENTIDAD, deberá ejecutar pruebas de aceptación que acrediten, como mínimo: a) su correcto estado operativo; b) su integración efectiva dentro de la solución ofertada; c) la cobertura de mantenimiento, soporte y garantía; d) la validación de vigencia tecnológica y estado de soporte; e) el cumplimiento de los niveles de disponibilidad, desempeño y continuidad exigidos.
	S11.	Plataforma SOAR (como parte del servicio SOC 24x7) S11.1. Objeto La ENTIDAD requiere complementar los servicios de seguridad y garantizar la automatización, orquestación y respuesta a incidentes de ciberseguridad mediante una plataforma tipo SOAR (Security Orchestration, Automation and Response), integrada al servicio SOC 24x7 provisto por el PROVEEDOR, con el fin de mejorar la eficiencia y efectividad de la detección, análisis, contención, erradicación, recuperación (restore) y mejora continua. S11.2. Alcance del servicio S11.2.1. El PROVEEDOR debe proveer y operar 24x7 el servicio de SOC, incluyendo las capacidades de SIEM y SOAR, y debe suministrar un Equipo de Respuesta a Incidentes (IRT) completo, suficiente e idóneo para atender integralmente los incidentes de ciberseguridad, sin dependencia operativa del CSIRT o IRT interno de la ENTIDAD. S11.2.2. El PROVEEDOR es responsable, como mínimo, de las fases de detección y análisis, contención, erradicación, recuperación o restore, actividades post-incidente, documentación del caso, análisis de causa raíz cuando aplique y lecciones aprendidas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S11.2.3. El despliegue del componente SOAR podrá ser on-premise, en nube o híbrido. En cualquiera de estas modalidades, el PROVEEDOR debe garantizar equivalencia funcional, seguridad, capacidad de auditoría, retención, disponibilidad, continuidad operativa, integridad de la información y cumplimiento de los requisitos establecidos por la ENTIDAD.

S11.3. ITIL estricto y gestión de casos en ITSM institucional

S11.3.1. El ITSM institucional de la ENTIDAD, ya sea el actualmente implementado o el que lo reemplace durante la ejecución contractual, será el único sistema oficial de registro para la gestión ITIL estricta de Incidente, Problema y Cambio, incluyendo estados, SLA, aprobaciones, evidencias, trazabilidad y cierre formal. En caso de discrepancia entre los registros del SOAR, SIEM o ITSM, prevalecerá el ITSM institucional para efectos de control contractual, supervisión, medición de niveles de servicio y auditoría.

S11.3.2. El SOAR debe integrarse con el ITSM institucional para, como mínimo:

a) Crear automáticamente tickets de Incidente y tareas asociadas y, cuando aplique, registros o tickets de Problema y de Cambio, incluido Cambio de Emergencia.
b) Sincronizar bidireccionalmente el identificador cruzado del caso entre SOAR, SIEM e ITSM, así como estados, severidad, prioridad, bitácora, comentarios, evidencias y demás metadatos definidos por la ENTIDAD.
c) Garantizar idempotencia, evitando la duplicación de tickets o acciones.
d) Implementar mecanismos de colas, reintentos controlados y alertamiento ante fallas de integración.
e) Mantener trazabilidad completa de las sincronizaciones y de los errores o inconsistencias presentados.

S11.3.3. Cambio de ITSM

Si la ENTIDAD sustituye o migra su ITSM durante la ejecución contractual, el PROVEEDOR debe adaptar la integración del SOAR y de los componentes relacionados al nuevo ITSM en un plazo máximo de treinta (30) días calendario, sin afectar la prestación del servicio 24x7. Cuando la ENTIDAD lo exija, el PROVEEDOR deberá soportar operación paralela durante el periodo de transición.

S11.4. Usuarios y roles de la plataforma SOAR

La plataforma SOAR deberá soportar como mínimo diez (10) usuarios concurrentes dentro del ecosistema operacional SOC-SIEM-SOAR. La solución deberá permitir la asignación configurable de roles mediante RBAC, incluyendo como mínimo administrador, editor o desarrollador de playbooks, analista u operador y usuario de consulta o auditoría.

No se establece una distribución fija por rol. El PROVEEDOR debe incluir todo el licenciamiento necesario para garantizar la operación

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

concurrente, la segregación de funciones, la administración, edición, prueba y ejecución de playbooks, la gestión de incidentes y la auditoría durante toda la vigencia contractual.

Cuando el fabricante utilice un modelo de licenciamiento diferente al de usuarios concurrentes, el OFERENTE deberá acreditar una capacidad funcional equivalente o superior, sin restricciones operativas para los perfiles definidos.

S11.5. Capacidades mínimas del SOAR

S11.5.1. Ingesta y normalización

El SOAR debe recibir alertas desde el SIEM y otras fuentes mediante API, syslog,webhook u otros mecanismos equivalentes, normalizarlas, deduplicarlas, agruparlas y correlacionarlas para su gestión.

S11.5.2. Enriquecimiento

El SOAR debe enriquecer automáticamente incidentes con contexto de activos, usuarios, IOC, CTI y demás información relevante, manteniendo trazabilidad de las fuentes consultadas.

S11.5.3. Triage y priorización

El SOAR debe asignar severidad/prioridad con reglas configurables y evidenciables en reportes.

S11.5.4. Playbooks y control humano

El SOAR debe ejecutar playbooks con condiciones, bifurcaciones, reintentos, reglas de escalamiento y control “human-in-the-loop” para acciones disruptivas.

Los playbooks SOAR podrán operar automáticamente para escenarios y acciones previamente aprobados por la ENTIDAD. Las acciones que puedan afectar servicios misionales, activos críticos, cuentas privilegiadas, evidencia digital o la continuidad operativa deberán incorporar aprobación humana.

Los casos sujetos a aprobación deberán incluir medidas preventivas, temporales o compensatorias previamente autorizadas. La solicitud de aprobación no constituye por sí sola contención efectiva.

Toda actuación deberá conservar trazabilidad en SIEM/SOAR e ITSM, incluyendo las marcas temporales de clasificación, activación del playbook, aprobación cuando aplique, acción ejecutada y resultado obtenido.

S11.5.5. Versionado y auditoría

El SOAR debe mantener versionado, auditoría y capacidad de reversión o rollback de playbooks, configuraciones (quién/qué/cuándo) y registrar cada acción (manual o automática) en bitácora.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S11.6. Respuesta multiplataforma e integraciones mínimas

S11.6.1. El SOAR debe integrarse, como mínimo, con herramientas o dominios de EDR/XDR, Firewall o controles de red, correo electrónico, IAM, cloud y SSE, incluyendo según aplique ZTNA, SWG, CASB y DLP, y debe permitir la orquestación de acciones automáticas o asistidas dejando evidencia verificable de su ejecución.

S11.6.2. Como mínimo, el PROVEEDOR debe garantizar la capacidad de ejecutar o asistir, según corresponda, las siguientes acciones:
a) En EDR/XDR: aislamiento de host, cuarentena y bloqueo por IOC, hash u otros indicadores.
b) En red o firewall: bloqueo de IP, dominio o URL, creación de reglas temporales con expiración controlada y reversión.
c) En correo electrónico: cuarentena o purga de mensajes, bloqueo de remitentes, URLs o elementos maliciosos.
d) En IAM: deshabilitación de cuentas, revocación de sesiones o tokens, restablecimiento de credenciales y forzado de MFA.
e) En cloud y SSE: revocación de llaves, ajuste de políticas, aislamiento de recursos y bloqueos en SWG, ZTNA, CASB o DLP, según corresponda.

S11.6.3. El PROVEEDOR debe monitorear, medir y reportar de forma continua la salud de las integraciones del SOAR, incluyendo como mínimo latencia, disponibilidad, fallas, cola de procesamiento, reintentos, errores de ejecución y tiempos de sincronización.

S11.7. Disparadores ITIL y gestión de emergencia

La plataforma y el servicio deberán operar bajo ITIL estricto conforme a las siguientes reglas mínimas:
a) Se debe crear automáticamente un Incidente en el ITSM institucional cuando la severidad sea Alta o Crítica, cuando un playbook ejecute acciones de contención o mitigación, o cuando exista impacto confirmado.
b) Se debe crear o proponer un Problema cuando existan recurrencias, causa raíz probable o necesidad de corrección permanente.
c) Se debe gestionar un Cambio para toda modificación persistente en Firewall, IAM, SSE, cloud, políticas o cualquier otro control bajo gobierno de cambios.
d) Solo para incidentes Críticos se podrán ejecutar acciones urgentes de contención sin aprobación previa, siempre que se registren en el ITSM institucional dentro de los quince (15) minutos siguientes, incluyendo justificación, evidencia técnica, impacto y plan de reversión.
e) Cuando la acción de emergencia implique una modificación persistente o impacto operativo, el PROVEEDOR debe generar el correspondiente Cambio de Emergencia y tramitar su post-aprobación conforme a los tiempos y lineamientos definidos por la ENTIDAD.
f) El PROVEEDOR deberá gestionar los cambios de acuerdo con lo establecido por la ENTIDAD para tal fin y mediante el comité de cambios ya establecido.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S11.8. Medición oficial, SLA y reportes

S11.8.1. Medición oficial: los SLA se medirán con timestamps del ITSM institucional (system of record); el SOAR y el SIEM aportarán la evidencia técnica asociada.

S11.8.2. El PROVEEDOR debe reportar mensualmente como mínimo: MTTD, MTTR, cumplimiento SLA por severidad, volumen alertas, incidentes, problemas y cambios, tasa de automatización, salud de integraciones, backlog y acciones de mejora y demás indicadores que defina la ENTIDAD.

S11.8.3. Informe por incidente: Por cada incidente atendido, el PROVEEDOR debe entregar un informe que incluya como mínimo cronología del evento, alcance, impacto, evidencias, acciones ejecutadas, medidas de contención, actividades de restore o recuperación, validación posterior, análisis de causa raíz cuando aplique y lecciones aprendidas.

S11.8.4. Informes ad-hoc: La ENTIDAD podrá solicitar informes ad hoc o reportes adicionales sobre casos, tendencias, integraciones, playbooks, trazabilidad, estado de acciones o cualquier otro aspecto del servicio, y el PROVEEDOR deberá suministrarlos con el detalle, formato, oportunidad y trazabilidad definidos por la ENTIDAD.

S11.9. Retención, integridad y exportación

S11.9.1. El PROVEEDOR debe garantizar una retención mínima de treinta y seis (36) meses para logs del SIEM, bitácoras del SOAR, evidencias, reportes, auditorías y demás registros asociados al servicio, los cuales deberán ser consultables y exportables durante todo el periodo contractual.

S11.9.2. Protección e integridad: los registros deberán estar protegidos contra acceso no autorizado, modificación o borrado, preferiblemente mediante mecanismos de inmutabilidad o WORM, o controles equivalentes aceptados por la ENTIDAD.

S11.10. Seguridad del SOAR/SIEM y continuidad

El PROVEEDOR debe garantizar como mínimo RBAC, MFA, segregación de funciones, trazabilidad de acciones administrativas y operativas, cifrado en tránsito y en reposo, respaldo, recuperación, continuidad operativa y la disponibilidad del servicio establecida en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

S11.11. Cumplimiento de privacidad y tratamiento de datos

El PROVEEDOR debe cumplir integralmente el régimen aplicable en materia de protección de datos personales, seguridad de la información, confidencialidad y tratamiento de la información, incluyendo las condiciones de transferencia, acceso, custodia, protección y uso autorizado cuando aplique.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S11.12. Infraestructura SOAR existente de la ENTIDAD

La ENTIDAD cuenta actualmente con una plataforma SOAR compuesta por dos (2) instancias FortiSOAR con licenciamiento, soporte y garantía hasta el 21 de diciembre de 2026, instaladas sobre dos (2) servidores marca DELL modelo POWEREDGE R540 con soporte y garantía hasta el 30 de enero de 2027, ubicados uno (1) en Bogotá y uno (1) en Cali.

A potestad del PROVEEDOR, dichos componentes podrán ser utilizados total o parcialmente dentro de la arquitectura técnica propuesta para la prestación del servicio, siempre que su incorporación sea técnicamente viable, compatible con la solución ofertada y permita cumplir integralmente con los niveles de servicio, capacidades funcionales, requerimientos técnicos, de seguridad, continuidad y de aseguramiento definidos en el proceso.

La decisión de utilizar o no la infraestructura existente es responsabilidad del PROVEEDOR, sin que ello releve el cumplimiento total del objeto contractual ni de los requisitos exigidos para el servicio SOC y para el componente SOAR.

Las referencias a Fortinet, FortiSOAR, DELL y POWEREDGE corresponden exclusivamente a la identificación de la infraestructura actualmente disponible en la ENTIDAD y no constituyen una exigencia de marca para los componentes nuevos, alternativos o de reemplazo que proponga el OFERENTE.

S11.13. Mantenimiento, soporte y garantía de la infraestructura existente

En caso de que el PROVEEDOR decida incorporar dentro de su arquitectura propuesta cualquiera de los componentes SOAR actualmente disponibles en la ENTIDAD, debe asumir durante toda la ejecución del contrato y sin costo adicional para la ENTIDAD, como mínimo, las siguientes obligaciones respecto de dichos componentes:
a) mantenimiento preventivo, correctivo y evolutivo que resulte aplicable;
b) soporte técnico especializado;
c) garantía y gestión de garantía frente al fabricante o canal autorizado, cuando corresponda;
d) reposición de partes, reemplazo de componentes defectuosos;
e) licenciamiento, actualización, parcheo, administración, operación, revisión de estado operativo y demás actividades necesarias para asegurar su adecuada operación y su correcto funcionamiento durante toda la ejecución contractual.

S11.14. Diagnóstico técnico inicial obligatorio

El PROVEEDOR debe realizar, dentro del plazo de alistamiento definido por la ENTIDAD, un diagnóstico integral del hardware, software, sistema operativo, base de datos, licenciamiento, versiones, capacidad, desempeño, conectores, playbooks, integraciones, seguridad, estado de soporte y demás componentes de la plataforma SOAR existente, y debe entregar a la supervisión un informe técnico

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

con hallazgos, riesgos, brechas, recomendaciones y plan de tratamiento.

S11.15. Validación de vigencia tecnológica y de soporte

El PROVEEDOR debe verificar y garantizar, previo a la puesta en marcha y durante la ejecución contractual, que ninguno de los componentes utilizados en la arquitectura propuesta, ya sean existentes o suministrados por él, se encuentre en estado EOL (End of Life), EOS (End of Support), EOSL (End of Service Life) o situación equivalente que comprometa su soporte, mantenimiento, actualización, operación segura o continuidad durante la ejecución del contrato. Para ello, deberá presentar evidencia documental emitida por el fabricante o por canal autorizado sobre la vigencia de soporte de cada componente incorporado al servicio.

S11.16. Reemplazo obligatorio por obsolescencia o fin de soporte

Si durante la ejecución contractual cualquiera de los componentes utilizados para la prestación del servicio entra en estado EOL, EOS, EOSL o condición equivalente, o si su continuidad compromete la seguridad, disponibilidad, mantenibilidad, capacidad de soporte o continuidad operativa del servicio, el PROVEEDOR debe, sin costo adicional para la ENTIDAD, suministrar, instalar, configurar, migrar, poner en funcionamiento y dejar estabilizado un componente nuevo de iguales o superiores características técnicas funcionales, de capacidad, desempeño, disponibilidad y compatibilidad, garantizando la continuidad del servicio y la no afectación material de la operación del SOC.

La sustitución debe incluir, cuando aplique, la migración, configuración, puesta en funcionamiento, pruebas, estabilización y transferencia operativa necesarias para mantener la integridad, disponibilidad y trazabilidad del servicio.

S11.17. Condiciones del reemplazo

Todo reemplazo de componentes deberá garantizar plena compatibilidad con la arquitectura propuesta, continuidad del servicio, integridad de la información, preservación de configuraciones, conectores, playbooks, evidencias, registros históricos y trazabilidad aplicable. El reemplazo no podrá ocasionar una interrupción injustificada del servicio ni una disminución de las capacidades exigidas por la ENTIDAD.

S11.18. Gestión de transición y cambio

Las actividades de migración, reemplazo, actualización mayor o sustitución de componentes deberán ejecutarse bajo plan formal de transición, análisis de impacto, gestión de cambios, plan de reversión, pruebas funcionales, pruebas de rendimiento, validación de integraciones, estabilización y entrega de evidencias al supervisor del contrato.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S11.19. No utilización de la plataforma existente Si el PROVEEDOR decide no utilizar la infraestructura SOAR existente de la ENTIDAD, ello no lo exonera del cumplimiento integral del objeto contractual ni de los niveles de servicio exigidos. En tal caso, el PROVEEDOR debe suministrar, implementar, soportar y operar por su cuenta y riesgo, y sin costo adicional para la ENTIDAD, todos los componentes de hardware, software, licenciamiento, respaldo, continuidad, seguridad e integración necesarios para garantizar capacidades iguales o superiores a las definidas por la ENTIDAD. S11.20. Condición de componentes nuevos Todos los componentes nuevos o de reemplazo que se suministren para garantizar la prestación del servicio deberán ser originales, nuevos, no reacondicionados, no remanufacturados, estar soportados por el fabricante y cumplir con las especificaciones técnicas, funcionales, de capacidad, seguridad y compatibilidad exigidas por la ENTIDAD. S11.21. Riesgo a cargo del PROVEEDOR La decisión del PROVEEDOR de utilizar o no la infraestructura existente de la ENTIDAD es de su exclusiva responsabilidad y no podrá ser invocada como causa de sobrecostos, mayores tiempos de implementación, restricciones técnicas, disminución funcional, incumplimiento de niveles de servicio o solicitud de reconocimiento económico adicional. S11.22. Plan de salida Al finalizar el contrato, el PROVEEDOR debe entregar a la ENTIDAD la exportación completa de los tickets registrados en ITSM, evidencias, bitácoras, reportes, configuraciones, documentación y demás registros asociados al servicio, de conformidad con la política de retención definida, garantizando continuidad, integridad, auditabilidad y posibilidad de consulta posterior.
	S12.	Servicio de NDR (Network Detection & Response) S12.1. Objeto El PROVEEDOR debe suministrar, implementar, operar y mantener un servicio de NDR 24x7 (integrado al SOC como servicio 24x7), que permita la recolección, análisis, detección, investigación, priorización, contención/mitigación y soporte de respuesta ante incidentes de ciberseguridad basados en telemetría de red, para ambientes On-premise, nube y/o híbridos, El dimensionamiento del servicio NDR debe ser realizado por EL PROVEEDOR, considerando el universo de activos y segmentos de red, sedes, dispositivos definidos por la ENTIDAD. Dicho universo es dinámico y puede variar durante la ejecución contractual; por lo tanto, la solución debe ser escalable y garantizar cobertura efectiva en

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

entornos on-premise, nube e híbridos, sin depender de un número fijo de IPs o sitios.

S12.1.1. El servicio debe cubrir, como mínimo:

- Visibilidad de tráfico de red, flujos, metadatos, DNS y eventos de seguridad de red.
- Detección de amenazas mediante firmas + analítica de comportamiento + detección de anomalías.
- Investigación con evidencia de red (flujos/metadatos y, cuando aplique, captura de paquetes).
- Capacidad de respuesta (manual, semi□automática o automática preaprobada) integrada con controles de red y seguridad (FW/WAF/SSE/ZTNA, EDR, IAM, cloud).

S12.2. Alcance y cobertura mínima

S12.2.1. Cobertura operacional

S12.2.1.1. El servicio debe operar 24x7, con turnos y capacidad suficiente para atender la demanda.

S12.2.1.2. El servicio debe incluir como mínimo niveles de atención establecidos en el anexo de ANS establecidos para cada servicio y un esquema de escalamiento y comunicación definido con la ENTIDAD.

S12.2.2. Cobertura de entornos y segmentos

S12.2.2.1. On-premise. Debe cubrir:

- Red de usuarios, data center, DMZ, redes de servidores, redes de administración, y segmentos críticos definidos por la ENTIDAD.
- Tráfico norte□sur (hacia/desde Internet) y este-oeste (lateral dentro del DC y entre VLANs/zonas).

S12.2.2.2. Nube / multi-cloud. Debe cubrir, según aplique:

- Tráfico entre Redes virtuales, subredes, grupos de seguridad y controles equivalentes de cada proveedor cloud, incluidos VNET, VPC, NSG o SG cuando existan en el entorno institucional, entre cargas (VM, contenedores, PaaS cuando aplique), y hacia Internet.
- Integración con mecanismos nativos de cada nube para telemetría (flow logs, traffic mirroring, logs de DNS y balanceadores), sin dependencia de un único proveedor.

S12.2.2.3. Híbrido. Debe cubrir tráfico entre on-premise y nube (VPN, Enlaces privados o servicios de interconexión dedicada con proveedores de nube, o mecanismos funcionalmente equivalentes), incluyendo detección de movimiento lateral y exfiltración.

S12.2.3. Universo de activos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S12.2.3.1. La ENTIDAD definirá el universo inicial de activos/segmentos críticos (vía CMDB, inventarios o listados).

S12.2.3.2. El PROVEEDOR debe proponer un plan de instrumentación (sensores/puntos de observación) para lograr cobertura efectiva y validable.

S12.2.3.3. La solución NDR podrá utilizar como fuentes de telemetría los flujos, metadatos, eventos IPS, registros DNS, aplicaciones y sesiones generados por los NGFW, CPE SD-WAN, switches, controladores y demás componentes de red disponibles. No se exigirá el despliegue de sensores físicos dedicados en todas las sedes.

El PROVEEDOR deberá complementar esta telemetría con sensores físicos, virtuales, cloud o mecanismos equivalentes en datacenters, nubes, segmentos críticos y puntos donde se requiera inspección profunda o se identifiquen brechas de visibilidad. La arquitectura deberá garantizar cobertura efectiva, ausencia de puntos ciegos relevantes e integración con el servicio SOC.

S12.3. Arquitectura y modelos de despliegue

S12.3.1. La solución del servicio NDR puede operar en modalidad on-premise, nube o híbrida, siempre que garantice capacidades equivalentes, seguridad, auditoría, retención y disponibilidad.

S12.3.2. La instrumentación debe contemplar una o varias de estas fuentes (según aplique), evitando dependencia exclusiva de una sola:

- TAP/SPAN/port□mirror para tráfico on□premise.
- Sensores virtuales en nube.
- Flow logs (VPC/VNET/NSG o equivalentes), DNS logs, logs de balanceadores/proxies y telemetría de red nativa cloud.
- Integraciones por API/webhook/syslog con plataformas de red y seguridad.

S12.3.3. El PROVEEDOR debe asegurar que los componentes críticos del servicio NDR (sensores, colectores y pipeline de análisis) cuenten con mecanismos de resiliencia que garanticen la continuidad del servicio y la no pérdida de telemetría ante la falla de un componente. No se exige un esquema específico de alta disponibilidad; se aceptarán los mecanismos propios de la solución ofertada, tales como redundancia funcional, almacenamiento temporal local, recuperación automática o tolerancia a fallos, que deberán demostrarse mediante documentación oficial del fabricante y pruebas de aceptación. El alcance de estos mecanismos por punto de captura se definirá en el diseño aprobado por la ENTIDAD.

S12.4. Capacidades mínimas de detección (funcionales y verificables)

S12.4.1. Detección por comportamiento y anomalías

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S12.4.1.1. El servicio debe incluir analítica de comportamiento y/o anomalías para:

- Detección de movimiento lateral (escaneo interno, enumeración, SMB/RDP/WinRM anómalo,etc).
- Comando y control (C2), beaconing, túneles, DNS anomalías.
- Exfiltración (volumen, destinos raros, patrones temporales, protocolos atípicos).
- Actividad sospechosa de credenciales (pass□the□hash/pivoting observado desde red cuando aplique).

S12.4.2. Análisis de Tráfico Cifrado

S12.4.2.1. La solución debe soportar análisis de tráfico cifrado mediante metadatos (SNI, certificados, fingerprints, patrones de sesión) y detecciones basadas en comportamiento, sin requerir inspección TLS para operar.

S12.4.2.2. Si la ENTIDAD dispone de inspección TLS en SSE/Proxy, el NDR debe permitir correlación con esa evidencia (cuando sea autorizado).

S12.4.3. Inteligencia de Amenazas e IoCs

S12.4.3.1. Integración con fuentes de inteligencia (IoCs IP/dominio/URL/hashes cuando aplique), con actualización periódica y trazabilidad de uso en casos.

S12.4.3.2. Capacidad de listas permitir/denegar y manejo de falsos positivos (afinamiento controlado y auditable).

S12.5. Evidencia, investigación y análisis forense de redes

S12.5.1. Evidencia consultable

S12.5.1.1. La solución debe permitir investigar incidentes con:

- Flujos y metadatos enriquecidos (quién, qué, cuándo, dónde; usuario/activo/segmento).
- Búsquedas por IP, host, usuario, dominio, puerto, protocolo, ASN/Geo, etc.
- Línea de tiempo de actividad y relaciones (gráficos de conexiones/paths) cuando aplique.

S12.5.2. Captura de paquetes (PCAP) — opcional y por tramos

S12.5.2.1. Si la ENTIDAD lo requiere, el PROVEEDOR debe ofrecer capacidad de captura de paquetes (selectiva o por eventos), dimensionada por tramos (retención, volumen, puntos de captura), sin imponerla como requisito universal.

S12.5.2.2. Para PCAP se deben establecer políticas de privacidad, minimización y acceso restringido, acorde con la normatividad aplicable.

S12.6. Integraciones (SASE/SSE + SOC + cloud)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S12.6.1. Integración con SOC/SIEM/SOAR/ITSM/CMDB y Observabilidad

S12.6.1.1. SIEM/SOC. El NDR debe integrarse con el SIEM del SOC como servicio para enviar alertas, evidencias y contexto (API/syslog/webhook o equivalente).

S12.6.1.2. SOAR. Debe habilitar disparadores para playbooks (contención, bloqueo, aislamiento) con control humano cuando aplique.

S12.6.1.3. ITSM: Todo incidente confirmado o alertas definidas por la ENTIDAD deben generar ticket en ITSM institucional con evidencia y trazabilidad.

S12.6.1.4. CMDB: La solución debe enriquecerse con criticidad, propietario, servicio y metadatos del CI, y vincular tickets a CI.

S12.6.2. Integraciones mínimas con controles (respuesta)

S12.6.2.1. El servicio debe permitir acciones de respuesta (manual / aprobada / automática preaprobada) integrándose, directamente o a través del SOAR, como mínimo con:

- Firewall / controles de red (bloqueo IP/dominio/URL, reglas temporales con expiración).
- SSE/SWG/ZTNA/CASB/DLP cuando aplique (bloqueos, políticas, aislamiento de usuario/sesión).
- EDR/XDR (aislamiento endpoint, cuarentena, bloqueo por IOC/hash) cuando aplique.
- IAM/Directorio (deshabilitar cuenta, revocar sesión, forzar MFA/reset) cuando aplique.
- Cloud (revocar llaves, aislar recursos, ajustar SG/NSG, cuarentena de instancias) cuando aplique.

S12.6.2.2. Gobernanza. Las acciones disruptivas deben ser human in the loop o aprobadas en ITSM, excepto escenarios de emergencia previamente definidos.

S12.7. Desempeño, dimensionamiento y escalabilidad (enfoque verificable)

S12.7.1. Dimensionamiento basado en tráfico real

S12.7.1.1. El PROVEEDOR debe presentar un dimensionamiento propuesto basado en:

- Medición inicial (baseline) de tráfico por segmento/punto de captura,
- Estimación de crecimiento,
- Capacidad por sensor/colector (throughput) y almacenamiento requerido.

S12.7.1.2. Para evitar ambigüedad, la propuesta debe incluir:

- Capacidad de procesamiento sostenida y pico por punto de observación,
- Latencia de detección/alertamiento,
- Número de sensores/instancias y redundancia.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S12.7.2. Latencia

S12.7.2.1. La latencia máxima de generación de alerta (desde recepción del dato de red hasta creación del caso), por severidad, será la establecida en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

S12.7.3. Escalabilidad por tramos: La escalabilidad debe ofrecerse mediante modelo por tramos (sensores, throughput, retención, conectores, almacenamiento), verificable y transparente.

S12.8. Continuidad de telemetría y calidad de datos (SLO)

S12.8.1. El PROVEEDOR debe implementar mecanismos de buffer/store□and□forward, colas, reintentos y monitoreo de salud de sensores y pipelines.

S12.8.2. Se exigirá un SLO medible de disponibilidad y entrega de telemetría, conforme a los niveles de servicio establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio, con reporte mensual de:
- Telemetría recibida vs esperada (por punto/sensor),
- Brechas (gaps), causas raíz y tiempos de recuperación,
- Acciones correctivas.

S12.9. Retención, custodia e integridad

S12.9.1. Retención mínima

S12.9.1.1. El servicio debe conservar como mínimo:
- Metadatos/alertas/evidencias: mínimo 36 meses consultables.
- Reportes y bitácoras operativas: mínimo durante toda la vigencia contractual y el periodo de retención.
- Evidencia asociada a incidentes: conservarse según requerimientos probatorios/auditoría.

S12.9.2. Integridad y cadena de custodia

S12.9.2.1. Los registros deben protegerse contra modificación o borrado no autorizado, preferiblemente con almacenamiento inmutable/WORM o controles equivalentes (hashing, control de borrado, segregación de funciones, auditoría).

S12.9.2.2. Debe existir procedimiento de exportación controlada para auditoría o uso probatorio.

S12.10. Seguridad de la plataforma

S12.10.1. Control de acceso con RBAC, MFA, segregación de funciones y auditoría completa (quién/qué/cuándo).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S12.10.2. Cifrado en tránsito (TLS) y en reposo; gestión segura de llaves/secretos.

S12.10.3. Separación lógica de datos de la ENTIDAD (tenant/espacio segregado) y prevención de exposición a terceros.

S12.10.4. Disponibilidad: El servicio debe cumplir la disponibilidad establecida en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

S12.11. Gestión de incidentes, SLAs y operación 24x7

S12.11.1. El servicio debe operar un proceso formal de respuesta a incidentes (detección, análisis, contención, erradicación, recuperación, lecciones aprendidas), integrable con el SOC como servicio y el ITSM institucional.

S12.11.2. Matriz de severidades S1—S4 definida con la ENTIDAD y ponderada por criticidad CMDB.

S12.11.3. Niveles de servicio. Los tiempos de atención, notificación y contención por severidad, su método de medición y las penalidades aplicables son los definidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

S12.12. Entregables y reportes

S12.12.1. Reporte mensual con KPIs:
- MTTD, MTTR, cumplimiento SLA por severidad,
- Volumen: detecciones/alertas/casos confirmados,
- Top casos de uso, afinamientos y falsos positivos,
- Cobertura por segmento, salud de sensores e integraciones.

S12.12.2. Reporte por incidente (cuando aplique):
- Línea de tiempo (Timeline), impacto, evidencia (metadatos/PCAP si aplica), acciones ejecutadas, verificación de restore, RCA y lecciones aprendidas.

S12.12.3. Reportes ad hoc: la ENTIDAD puede solicitar reportes adicionales relacionados con auditorías, investigaciones o control interno.

S12.13. Pruebas de aceptación (criterios mínimos)

Como condición de aceptación (por fases), el PROVEEDOR debe ejecutar y documentar pruebas que evidencien:

S12.13.1. Cobertura e instrumentación
- Instalación/activación de sensores o fuentes cloud en segmentos definidos.
- Evidencia de recolección efectiva (volumen/latencia) por punto de observación.

S12.13.2. Detección

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Simulación controlada de al menos 8 escenarios: escaneo lateral, beaconing/DNS anómalo, exfiltración simulada, conexión a dominio/IP malicioso (laboratorio).
- Evidencia de alertas con severidad y contexto (CI/usuario/segmento).

S12.13.3. Integración SOC/ITSM/CMDB/Observabilidad

- Generación de ticket en ITSM institucional con enlace a CI y evidencias.
- Correlación con SIEM/SOAR.

S12.13.4. Respuesta

- Ejecución controlada de al menos 3 acciones: bloqueo IP/dominio, aislamiento endpoint (si EDR), acción IAM/SSE (si aplica), con trazabilidad y aprobación cuando aplique.

S12.13.5. Calidad y continuidad

- Simulación de falla de enlace/sensor y evidencia de recuperación y reporte de gaps conforme SLO.

S12.14. Privacidad, tratamiento de datos y cumplimiento normativo

S12.14.1. El PROVEEDOR debe cumplir la normativa aplicable de protección de datos personales y confidencialidad, e implementar medidas técnicas y organizativas apropiadas.

S12.14.2. Cuando haya tratamiento/transferencia/encargo, debe documentarse el modelo y responsabilidades.

Documentación técnica exigida El PROVEEDOR debe entregar al inicio del contrato:

S12.14.3. Arquitectura propuesta (on□prem/nube/híbrida), puntos de observación, alta disponibilidad y seguridad, incluyendo descripción de equipos que conforman el servicio (marca, modelo, capacidades) de acuerdo con el anexo 1.1. sedes para conectar.

S12.14.4. Dimensionamiento (throughput, almacenamiento, retención), supuestos y márgenes de crecimiento.

S12.14.5. Alcance de integraciones (SIEM/SOAR/ITSM/CMDB, cloud, SSE, FW, EDR, IAM, Observabilidad) y plan de onboarding.

S12.14.6. Catálogo de casos de uso inicial + plan de mejora continua.

S12.14.7. Evidencia documental (datasheets/fichas técnicas) indicando página y párrafo donde se prueban las capacidades solicitadas.

S12.14.8. Matriz de cumplimiento (checklist) firmada por el OFERENTE.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S12.15. Plan de salida S12.15.1. Al finalizar el contrato, el PROVEEDOR debe entregar como minimo la exportación completa de: - Alertas/casos, evidencias, reportes y bitácoras del NDR, - Configuraciones y playbooks (si aplica), - Documentación de integración y operación (runbooks), garantizando continuidad, auditabilidad y transferencia ordenada del servicio.
	S13.	Servicio de Administración del Network Access Control (NAC) SERVICIO NAC (NETWORK ACCESS CONTROL) ON-PREMISE Y NUBE / HÍBRIDO — INTEGRADO AL SOC COMO SERVICIO S13.1. Objeto S13.1.1. El PROVEEDOR debe asumir la administración, operación y soporte del Servicio de Network Access Control (NAC) vigente, que permita identificar, autenticar, perfilar, autorizar, segmentar y aplicar postura (posture/compliance) a los dispositivos y usuarios que se conecten a la infraestructura tecnológica de la ENTIDAD, tanto en ambientes on-premise (LAN/WLAN/VPN) como en accesos a recursos en nube/SaaS mediante mecanismos equivalentes (integración con IAM/SSE/ZTNA/MDM), con el fin de reducir riesgos de intrusión, movimiento lateral y acceso no autorizado. S13.1.2. El PROVEEDOR debe garantizar la continuidad del servicio mediante la administración, operación, soporte, mantenimiento, actualización, afinamiento e implementación de mejoras y nuevas políticas sobre la plataforma NAC existente de la ENTIDAD. Hasta el 3 de marzo de 2029, el PROVEEDOR debe administrar la plataforma con el licenciamiento, soporte y garantía vigentes suministrados por la ENTIDAD. A partir del 4 de marzo de 2029 y hasta la finalización del contrato, el PROVEEDOR debe, a su discreción y bajo su exclusiva responsabilidad: (i) renovar y mantener vigentes el licenciamiento, soporte y garantía de la plataforma existente; o (ii) suministrar, implementar, migrar, operar, soportar y garantizar una nueva plataforma NAC que cumpla capacidades iguales o superiores a las exigidas en el presente numeral, sin afectar la continuidad del servicio ni generar costes adicionales para la ENTIDAD. S13.1.3. El servicio debe integrarse con el SOC como servicio 24x7 (SIEM/SOAR/ITSM/CMDB) para generación de casos, contención y trazabilidad, según gobernanza definida por la ENTIDAD. S13.2. Infraestructura NAC actualmente disponible en la ENTIDAD La ENTIDAD cuenta actualmente con un Servicio de NAC con la siguiente infraestructura NAC:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Plataforma HP ClearPass con licenciamiento, soporte y garantía vigentes hasta el 3 de marzo de 2029, con los siguientes componentes:
  - HPE Aruba Networking ClearPass Access License 10K Concurrent Endpoints E-LTU.
  - HPE Aruba Networking ClearPass Access License 25K Concurrent Endpoints E-LTU.
  - Dos (2) Aruba ClearPass Cx000V VM Appl E-LTU.
  - HPE Aruba Networking ClearPass - OnGuard License 25K Users E-LTU.
- La identificación de HPE Aruba Networking ClearPass corresponde exclusivamente a la descripción de la infraestructura existente de propiedad o bajo uso de la ENTIDAD y no constituye una exigencia de marca para la alternativa tecnológica que pueda implementarse a partir del 4 de marzo de 2029.

S13.2.1. Administración obligatoria de la plataforma existente y opción tecnológica posterior

Desde el inicio de la ejecución contractual y hasta el 3 de marzo de 2029, el PROVEEDOR debe asumir obligatoriamente la administración, operación, monitoreo, soporte, mantenimiento, actualización, afinamiento e integración de la plataforma NAC existente de la ENTIDAD, aprovechando el licenciamiento, soporte y garantía vigentes. Durante este periodo no será potestativo sustituir o dejar de utilizar la plataforma, salvo que exista una condición técnica, de seguridad, obsolescencia o continuidad debidamente sustentada y previamente autorizada por la ENTIDAD.

A partir del 4 de marzo de 2029, el PROVEEDOR podrá, a su discreción y bajo su exclusiva responsabilidad, continuar utilizando la plataforma existente mediante la renovación integral de su licenciamiento, soporte y garantía hasta la finalización del contrato, o implementar una nueva plataforma NAC. Cualquiera de las alternativas debe garantizar capacidades iguales o superiores, compatibilidad con la infraestructura institucional, continuidad del servicio, migración controlada, preservación de configuraciones, integraciones, registros y trazabilidad, y cumplimiento integral de los ANS y requisitos del servicio, sin costes adicionales para la ENTIDAD.

S13.2.2. Mantenimiento, soporte y garantía de los componentes existentes

El PROVEEDOR debe asumir durante toda la ejecución contractual la administración, operación y mantenimiento de los componentes NAC utilizados. Hasta el 3 de marzo de 2029, las coberturas de licenciamiento, soporte y garantía existentes serán aprovechadas por el PROVEEDOR, sin que ello limite su responsabilidad por la correcta prestación del servicio. A partir del 4 de marzo de 2029, si continúa utilizando la plataforma existente, debe renovar y mantener vigentes,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

por su cuenta y riesgo y sin coste adicional para la ENTIDAD, dichas coberturas hasta la finalización del contrato. Como mínimo, debe cumplir las siguientes obligaciones:
a) mantenimiento preventivo, correctivo y evolutivo que resulte aplicable;
b) soporte técnico especializado;
c) garantía y gestión de garantía frente al fabricante o canal autorizado, cuando corresponda;
d) reposición de partes, reemplazo de componentes defectuosos, cuando aplique;
e) administración, operación, monitoreo, actualización, parcheo, revisión de estado operativo y demás actividades necesarias para asegurar el correcto funcionamiento durante toda la ejecución contractual; y, a partir del 4 de marzo de 2029, cuando se mantenga la plataforma existente, renovación y vigencia continua del licenciamiento, soporte y garantía hasta la finalización del contrato.

S13.2.3. Validación de vigencia tecnológica y estado de soporte

El PROVEEDOR debe verificar y garantizar, previo a la puesta en marcha y durante la ejecución contractual, que los componentes utilizados en la arquitectura, sean existentes o suministrados por él, permanezcan en estado soportado por el fabricante y no se encuentren en EOL (End of Life), EOS (End of Support) o condición equivalente que comprometa su seguridad, mantenimiento, actualización, operación o continuidad. Esta obligación aplica igualmente a la alternativa tecnológica que el PROVEEDOR adopte a partir del 4 de marzo de 2029.
Dicha validación debe estar soportada documentalmente mediante evidencia del fabricante, canal autorizado o fuente oficial técnicamente verificable.

S13.2.4. Sustitución obligatoria por fin de vida

Si durante la ejecución del contrato cualquiera de los componentes incorporados a la solución entra en estado de EOL, EOS o condición equivalente, o si dicho estado se determina de forma sobreviniente, el PROVEEDOR debe, sin costo adicional para la ENTIDAD, realizar su sustitución por un componente nuevo de iguales o superiores características técnicas, funcionales, de capacidad, desempeño, disponibilidad y compatibilidad, garantizando la continuidad del servicio y la no afectación material de la operación.

La sustitución debe incluir, cuando aplique, la migración, configuración, puesta en funcionamiento, pruebas, estabilización y transferencia operativa necesarias para mantener la integridad, disponibilidad y trazabilidad del servicio.

S13.2.5. Condiciones del reemplazo

Todo reemplazo de componentes deberá garantizar plena compatibilidad con la arquitectura propuesta, continuidad del servicio, integridad de la información, preservación de configuraciones, conectores, evidencias, registros históricos y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

trazabilidad aplicable. El reemplazo no podrá ocasionar una interrupción injustificada del servicio ni una disminución de las capacidades exigidas por la ENTIDAD.

S13.2.6. Responsabilidad integral sobre la arquitectura propuesta

Es responsabilidad exclusiva del PROVEEDOR garantizar que la arquitectura NAC cumpla todos los requerimientos del proceso, incluidos capacidad, disponibilidad, seguridad, soporte, interoperabilidad, continuidad, retención, trazabilidad, auditabilidad y desempeño. Hasta el 3 de marzo de 2029 deberá administrar la plataforma existente; desde el 4 de marzo de 2029 deberá garantizar, a su elección, su renovación integral o la implementación de una nueva plataforma, y proponer las mejoras que resulten aplicables.

S13.2.7. Evaluación de compatibilidad y dimensionamiento

Si el PROVEEDOR decide utilizar componentes actualmente disponibles en la ENTIDAD, debe validar y documentar su compatibilidad, dimensionamiento, capacidad útil, desempeño y vida útil remanente respecto de la arquitectura propuesta y de la carga operativa del servicio, sin que ello implique limitación o reducción del alcance requerido por la ENTIDAD.

S13.2.8. Transición sin afectación material

Toda incorporación, sustitución, actualización, migración o retiro de componentes del NAC debe ejecutarse bajo procedimiento controlado, con gestión de riesgos, plan de reversión y evidencias, evitando afectación material de la operación del servicio, pérdida de eventos, pérdida de trazabilidad o indisponibilidad no autorizada.

S13.2.9. Implementación de una nueva plataforma a partir del 4 de marzo de 2029

Si el PROVEEDOR decide sustituir la plataforma NAC existente, deberá planificar, suministrar, implementar, migrar, probar, estabilizar, soportar y operar, por su cuenta y riesgo y sin coste adicional para la ENTIDAD, una nueva plataforma que incluya todos los componentes de hardware, software, licenciamiento, soporte, garantía, respaldo, continuidad, seguridad e integración necesarios. La nueva plataforma deberá acreditar capacidades iguales o superiores a las de la solución existente, garantizar la conservación y migración de la información y trazabilidad aplicables, y entrar en operación plenamente, a más tardar, el 3 de marzo de 2029, antes del vencimiento de las coberturas vigentes. Para ello, el PROVEEDOR deberá ejecutar las actividades con la debida antelación, garantizando la continuidad del servicio, sin interrupciones injustificadas ni degradación de los Acuerdos de Nivel de Servicio (ANS).

S13.2.10. Condición de componentes nuevos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Todos los componentes nuevos o de reemplazo que se suministren para garantizar la prestación del servicio deberán ser originales, nuevos, no reacondicionados, no remanufacturados, estar soportados por el fabricante y cumplir con las especificaciones técnicas, funcionales, de capacidad, seguridad y compatibilidad exigidas por la ENTIDAD.

S13.2.11. Riesgo a cargo del PROVEEDOR

La alternativa seleccionada por el PROVEEDOR a partir del 4 de marzo de 2029, ya sea renovar la plataforma existente o implementar una nueva, será de su exclusiva responsabilidad y no podrá invocarse como causa de sobrecostos, ampliación de plazos, restricciones técnicas, disminución funcional, interrupción del servicio, incumplimiento de ANS o reconocimiento económico adicional.

S13.3. Alcance y cobertura mínima

S13.3.1. Operación y servicio administrado

S13.3.1.1. El servicio NAC debe prestarse en modalidad administrada (Managed NAC) con atención 24x7, y con capacidad de escalamiento para eventos de seguridad coordinado con el SOC como servicio 24x7.

S13.3.1.2. El PROVEEDOR debe disponer de roles L1/L2/L3 para operación, soporte, afinamiento de políticas, troubleshooting y respuesta a incidentes relacionados con control de acceso.

S13.3.1.3. La solución debe proporcionar mecanismos de administración centralizada que permitan aplicar políticas consistentes de identidad, postura y control de acceso sobre los distintos métodos de conexión contemplados en el servicio, incluyendo acceso a la red, acceso remoto, VPN, ZTNA y SSE, garantizando trazabilidad, auditoría y sincronización de políticas entre los componentes involucrados.

S13.3.1.4. Se aceptarán soluciones funcionalmente equivalentes que garanticen administración centralizada, integración de identidades, auditoría y control granular de privilegios.

S13.3.2. Cobertura on□premise mínima

S13.3.2.1. Control de acceso a red cableada (LAN) y red inalámbrica (WLAN), incluyendo sedes, data center/zonas internas y redes críticas definidas por la ENTIDAD.

S13.3.2.2. Control de acceso para VPN o acceso remoto cuando aplique (por integración con el concentrador VPN, ZTNA o equivalente).

S13.3.3. Cobertura nube/híbrido mínima

S13.3.3.1. El NAC debe habilitar controles equivalentes para accesos a recursos en nube/SaaS, a través de integraciones con IAM (AD/Entra o equivalente), MDM, EDR/XDR, SSE/ZTNA y/o agentes de postura, de forma que:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Solo dispositivos identificados y conformes accedan a recursos críticos en nube/SaaS,
- Se aplique política de acceso basada en identidad, postura, riesgo y contexto,
- Se registre evidencia y trazabilidad consumible por SOC/SIEM.

S13.3.3.2. Si la ENTIDAD opera cargas IaaS (VMs/containers), el PROVEEDOR debe integrar el servicio con mecanismos de segmentación/controles de red cloud (NSG/SG, microsegmentación o equivalentes) para apoyar contención y reducción de movimiento lateral, sin exigir una marca específica.

S13.3.4. Conexiones simultaneas, licenciamiento y tipos de dispositivos

S13.3.4.1. El servicio debe contar con una plataforma con capacidad para al menos 30.000 conexiones simultaneas sobre las cuales mínimo 25.000 licencias permitan realizar postura sobre los dispositivos.

S13.3.4.2. El servicio debe cubrir como mínimo las categorías:
- Equipos corporativos (Windows/macOS/Linux),
- Dispositivos móviles (iOS/Android) cuando aplique,
- Impresoras, cámaras, IoT/OT y “dispositivos no administrados” (sin agente),
- Invitados/contratistas/BYOD (según políticas de la ENTIDAD).

S13.4. Capacidades funcionales mínimas del NAC

S13.4.1. Autenticación y autorización (AAA)

S13.4.1.1. El NAC debe soportar autenticación/autorización para acceso a red mediante estándares como:
- 802.1X (EAP□TLS y/o métodos equivalentes),
- MAB (MAC Authentication Bypass) para dispositivos que no soportan 802.1X (IoT/impresoras), con controles compensatorios,
- Portal cautivo/guest cuando aplique,
- Integración RADIUS/TACACS+ o equivalentes con infraestructura de red.

S13.4.1.2. Debe permitir políticas basadas en:
- Identidad (usuario/grupo),
- Tipo de dispositivo (perfil),
- Ubicación/segmento/SSID,
- Hora/condición,
- Criticidad/servicio (vía CMDB cuando aplique),
- Estado de postura/compliance.

S13.4.2. Perfilamiento y descubrimiento de dispositivos

S13.4.2.1. El NAC debe identificar y perfilar dispositivos con múltiples técnicas sin depender de un único método, DHCP/DNS, SNMP, ARP, HTTP user agents, TLS fingerprints, OUI, técnicas de descubrimiento y perfilamiento activo o pasivo mediante

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

sondas de red, identificación de servicios o mecanismos equivalentes donde aplique, etc.

S13.4.2.2. El NAC debe mantener un inventario dinámico (near real□time) de endpoints conectados y su estado (conectado/desconectado, segmento, IP/MAC, método de autenticación, perfil).

S13.4.3. Postura (posture/compliance) y evaluación de riesgo

S13.4.3.1. El NAC debe evaluar postura con verificación de:
- Estado de MDM (cumplimiento, cifrado, bloqueo, jailbreak/root),
- Estado de EDR/antimalware (instalado, activo, actualizado),
- Parcheo mínimo o versión OS (si la ENTIDAD lo exige),
- Configuraciones críticas (firewall host, cifrado de disco), de forma auditada.

S13.4.3.2. Debe permitir asignar un score/riesgo o clasificación de cumplimiento y aplicar políticas de acceso adaptativas (permitir, restringir, cuarentena, solo remediación).

S13.4.4. Segmentación y aplicación de políticas (enforcement)

S13.4.4.1. El NAC debe aplicar políticas de segmentación y control mediante mecanismos de enforcement soportados por la red:
- Asignación dinámica de VLAN/SSID,
- Listas de control de acceso dinámicas, atributos de autorización o mecanismos equivalentes soportados por la infraestructura de red,

- Etiquetas o atributos de seguridad para segmentación dinámica, mediante mecanismos estándar o funcionalmente equivalentes compatibles con la infraestructura de red utilizada por la ENTIDAD.

- Redirección a red de remediación/portal,
- Bloqueo/aislamiento controlado.

S13.4.4.2. Para nube/híbrido, el enforcement debe lograrse vía:
- Políticas de acceso en ZTNA/SSE (por postura/identidad),
- Integración con IAM (políticas de acceso adaptativo o condicional basadas en identidad, postura, riesgo y contexto),
- Controles de red cloud (SG/NSG/políticas) cuando aplique.

S13.4.5. Manejo de invitados, contratistas y BYOD

S13.4.5.1. El servicio debe soportar flujos de invitado/contratista:
- Registro, aprobación, tiempo de vida, expiración, segmentación de invitados separada de redes internas, Trazabilidad sobre quién invitó, cuándo, desde dónde.

S13.4.5.2. Para BYOD, debe soportar al menos una modalidad segura:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		- Onboarding mediante certificados/perfiles, o acceso restringido a recursos específicos vía ZTNA/SSE, evitando acceso a redes internas completas. S13.4.6. IoT/OT y dispositivos “sin agente” S13.4.6.1. El NAC debe permitir políticas específicas para IoT/OT: - Perfilamiento confiable, - Segmentación estricta (microsegmento/VLAN/ACL), - Detección de cambios (cambio de perfil o comportamiento de red), - Control de acceso basado en listas blancas donde aplique. S13.5. Integraciones (SOC/SIEM/SOAR/ITSM/CMDB + SASE/SSE) S13.5.1. Integración con directorios e identidad S13.5.1.1. Integración con Directorio Activo on□premise y/o Microsoft Entra ID para grupos/atributos y correlación de identidad. S13.5.1.2. Integración con PKI/certificados (si la ENTIDAD lo dispone o lo requiere para EAP□TLS), o propuesta del OFERENTE para aprovisionamiento seguro. S13.5.2. Integración con MDM y EDR/XDR S13.5.2.1. Integración con plataforma MDM (Intune u otra definida por la ENTIDAD) para consumir estado de cumplimiento. S13.5.2.2. Integración con EDR/XDR para consumir estado del agente y habilitar contención coordinada (aislamiento, cuarentena, bloqueo). S13.5.3. Integración con infraestructura de red S13.5.3.1. Integración con switches, controladores WLAN, concentradores VPN/ZTNA y/o soluciones de acceso, mediante protocolos estándares (RADIUS, SNMP, APIs) y conectores. S13.5.3.2. El OFERENTE debe declarar explícitamente el alcance de compatibilidad multi-marca y el plan de onboarding por fases. S13.5.4. Integración con SOC/SIEM/SOAR S13.5.4.1. El NAC debe enviar logs/eventos y alertas al SIEM del SOC como servicio (syslog/API/webhook o equivalente), con campos suficientes para correlación (usuario, endpoint, IP/MAC, ubicación, acción de política, motivo). S13.5.4.2. El NAC debe permitir acciones orquestadas al SOAR del SOC como servicio como cambiar VLAN/ACL, cuarentena,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

revocar acceso, bloquear endpoint, con gobernanza (aprobación/human-in-the-loop).

S13.5.5. Integración con ITSM institucional y CMDB

S13.5.5.1. Los incidentes/casos NAC definidos por la ENTIDAD deben generar tickets en ITSM institucional con evidencia.

S13.5.5.2. El NAC debe enriquecer y vincular con CMDB (CI correspondiente), y reportar inconsistencias (CI inexistente/atributos faltantes) como tickets de mejora.

S13.6. Seguridad, auditoría y segregación

S13.6.1. Acceso administrativo y operativo con MFA, RBAC, segregación de funciones y auditoría completa (quién/qué/cuándo).

S13.6.2. Cifrado en tránsito y reposo; gestión de llaves/secretos; registro de accesos y cambios.

S13.6.3. Segregación lógica de datos de la ENTIDAD (tenant/espacio segregado) en modalidad cloud/externa.

S13.7. Disponibilidad, continuidad y escalabilidad (control presupuestal)

S13.7.1. Alta disponibilidad

S13.7.1.1. La arquitectura NAC debe soportar alta disponibilidad de componentes críticos (AAA/RADIUS, policy engines, portales), con RTO/RPO definidos en la oferta.

S13.7.2. Escalabilidad por tramos

S13.7.2.1. La expansión debe ofrecerse por tramos verificables (número de endpoints, sedes, throughput RADIUS, integraciones, retención).

S13.7.2.2. La renovación o sustitución requerida para mantener el alcance y línea base contratados se entenderá incluida en el valor del servicio. Los crecimientos que excedan la línea base o los umbrales contratados se gestionarán mediante los precios unitarios por tramo establecidos.

S13.8. Políticas mínimas y gobierno de cambios (ITIL)

S13.8.1. El PROVEEDOR debe implementar políticas NAC mínimas acordadas con la ENTIDAD:

- Acceso corporativo (802.1X preferible),
- Acceso IoT/OT (MAB + segmentación),
- Acceso invitados/contratistas (portal/expiración/segmentación),
- Postura mínima (MDM/EDR),
- Cuarentena/remediación,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Excepciones controladas con vencimiento y aprobación.

S13.8.2. Los cambios de políticas con impacto deben gestionarse como cambio de acuerdo con los lineamientos del modelo de servicio de la FGN en ITSM institucional, con evidencia, aprobación y plan de reversión cuando aplique.

S13.9. Retención y trazabilidad

S13.9.1. El NAC debe retener logs/eventos, bitácoras de administración, evidencias y reportes por mínimo 36 meses, alineado con la política del SOC (consultables y exportables).

S13.9.2. Los registros deben protegerse contra modificación/borrado no autorizado, preferiblemente con controles de inmutabilidad/WORM o equivalentes verificables.

S13.10. SLAs y métricas

S13.10.1. Se deben definir SLAs medibles para:
- Tiempo de atención de incidentes NAC (alineado al SOC S1—S4),
- Tiempo de aprovisionamiento de nuevas sedes/segmentos/endpoints,
- Tiempo de implementación de políticas/cambios (por severidad y prioridad),
- Disponibilidad de la plataforma NAC.

S13.10.2. Reporte mensual mínimo:
- Endpoints vistos vs autorizados; top dispositivos por categoría,
- Eventos de denegación/cuarentena y sus causas,
- Cumplimiento posture; endpoints fuera de cumplimiento,
- Integraciones (salud RADIUS, latencias, colas, fallas),
- KPIs de operación: MTTR, volumen de tickets, backlog.

S13.11. Entregables y reportes

S13.11.1. Informe mensual de operación NAC y seguridad:
- Resumen ejecutivo + detalle técnico,
- Tendencias (compliance, accesos rechazados, IoT no reconocido),
- Cambios aplicados, excepciones otorgadas (con vencimiento),
- Recomendaciones de mejora y plan de hardening/segmentación.

S13.11.2. Informes ad-hoc: la ENTIDAD puede solicitar reportes adicionales (auditoría, investigación, control interno) con trazabilidad.

S13.12. Pruebas de aceptación

Como condición de aceptación por fases, el PROVEEDOR debe demostrar, al menos:

S13.12.1. Autenticación y segmentación

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- 802.1X operativo en un segmento piloto (LAN) con política por rol,
- WLAN corporativa con control de acceso,
- IoT/impresoras con MAB + segmentación segura,
- Invitados con portal y expiración.

S13.12.2. Postura
- Dispositivo compliant obtiene acceso normal,
- Dispositivo no compliant es redirigido a remediación o cuarentena,
- Evidencia de consumo de MDM/EDR (cuando aplique).

S13.12.3. Integración SOC/ITSM/CMDB
- Envío de eventos al SIEM y correlación básica,
- Ticket automático en ITSM institucional para eventos críticos (acceso no autorizado repetido, endpoint rogue, suplantación),
- Vinculación a CI/CMDB y enriquecimiento (criticidad/propietario).

S13.12.4. Respuesta
- Ejecución controlada de una acción de contención: cuarentena/cambio ACL/VLAN con trazabilidad y aprobación cuando aplique.

S13.12.5. Continuidad
- Prueba de failover/HA de componentes AAA/policy engine según arquitectura propuesta.

S13.13. Documentación técnica exigida

El PROVEEDOR deberá entregar la siguiente documentación al inicio del contrato:
- Arquitectura propuesta (on□prem/nube/híbrido), HA/DR, RTO/RPO,
- Plan de onboarding por fases (piloto → expansión),
- Matriz de compatibilidad multi□marca (switches/WLC/VPN/ZTNA),
- Integraciones (IAM/AD/Entra, MDM, EDR, SIEM/SOAR, ITSM/CMDB),
- Matriz de cumplimiento con evidencia (página/párrafo de fichas técnicas cuando aplique),
- Modelo de escalabilidad por tramos (endpoints/sedes/integraciones/retención).

S13.14. Plan de salida (exit plan)

Al finalizar el contrato, el PROVEEDOR debe entregar:
- Exportación de configuraciones (políticas, perfiles, reglas, excepciones y vencimientos),
- Inventario histórico de endpoints y reportes,
- Logs y evidencias conforme retención,
- Runbooks y documentación para transición operativa, garantizando continuidad y auditabilidad.

A partir del 4 de marzo de 2029, el PROVEEDOR podrá renovar y continuar operando la plataforma NAC existente o implementar una nueva plataforma, bajo las condiciones de equivalencia funcional,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		continuidad, seguridad, integración, soporte, garantía, trazabilidad y responsabilidad establecidas en los numerales precedentes.
	S14.	Servicio de Antimalware para Endpoint, para Servidores y para dispositivos de almacenamiento NAS con capacidades de XDR SERVICIO UNIFICADO DE PROTECCIÓN ANTIMALWARE (EPP/NGAV) + XDR Endpoints + Servidores + NAS — On□premise y Nube — Integrado al SOC como servicio 24x7 S14.1. Objeto S14.1.1. El PROVEEDOR debe suministrar, implementar, operar y mantener un servicio unificado de protección antimalware de nueva generación (EPP/NGAV) con capacidades XDR (Extended Detection and Response) para la Fiscalía General de la Nación, con el fin de prevenir, detectar, investigar, correlacionar y responder a amenazas (malware, ransomware, PUA/PUP, scripts maliciosos y técnicas comunes de intrusión) en ambientes on□premise, nube y/o híbridos. S14.1.2. El servicio debe cubrir, como mínimo, los siguientes activos: □ 26.000 endpoints (aprox.) de usuario. □ 500 servidores (aprox.): 250 Linux y 250 Windows Server. □ Dos (2) soluciones NAS Hitachi HNAS Platform 4060: una en Bogotá y una en Cali, con arquitectura detallada en S14.10. □ Workloads en nube (IaaS) (VM/instancias y recursos definidos por la ENTIDAD), incorporadas por fases. □ Nota: La cantidad de veintiséis mil (26.000) endpoints corresponde a la protección Antimalware + XDR de endpoints de usuario; adicionalmente, el servicio comprende quinientos (500) servidores Windows/Linux y la protección e integración de las soluciones NAS y de las cargas en nube indicadas en el presente numeral. Las cifras de treinta mil (30.000) usuarios previstas para el servicio SASE/SSE u otros servicios del presente anexo no constituyen cantidades de endpoints Antimalware/XDR ni generan activación o pago automático. Toda ampliación sobre las cantidades establecidas en el Formato de Oferta Económica requerirá solicitud y autorización previa de la ENTIDAD y el mecanismo contractual correspondiente. S14.1.3. El servicio debe estar asociado e integrado al SOC como servicio 24x7 (SIEM, SOAR, ITSM institucional y CMDB). S14.2. Alcance y modalidad del servicio S14.2.1. Servicio administrado (Managed Service). Incluye: diseño, despliegue por fases, políticas, operación, monitoreo, investigación, contención (según gobernanza), soporte, mejora continua y reportes. S14.2.2. Modelo operativo. Se alineará al SOC como servicio (L1/L2/L3 o equivalente) y al proceso formal de respuesta a incidentes (detección, análisis, contención, erradicación,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

recuperación y lecciones aprendidas), con trazabilidad en ITSM institucional.

S14.3. Compatibilidad de Sistemas Operativos

S14.3.1. Soporte mínimo requerido

El servicio debe cubrir antimalware y telemetría/acciones XDR (según aplique) para:

- Windows (Endpoints): Windows XP en adelante.
- Windows Server: Windows Server 2008 en adelante.
- macOS: Monterey en adelante.
- Linux (múltiples distribuciones): incluyendo como mínimo:
  - RHEL 6 en adelante.
  - CentOS 6 en adelante.

El servicio debe cubrir los sistemas operativos vigentes y legados identificados en la línea base institucional. Cuando una versión no sea soportada directamente por el agente o fabricante de la solución, el PROVEEDOR debe implementar controles compensatorios equivalentes, documentados, medibles y aprobados por la ENTIDAD.

S14.3.2. Matriz de soporte y limitaciones

El OFERENTE debe anexar una matriz por OS/versión indicando:

- Soporte con agente,
- Capacidades disponibles (prevención, telemetría, aislamiento, artefactos),
- Limitaciones y mitigaciones.

S14.3.3. Controles compensatorios para OS legacy

Para OS legados o fuera de soporte del fabricante del agente (posibles casos de XP/RHEL6/CentOS6), el PROVEEDOR debe garantizar protección equivalente verificable mediante controles compensatorios (uno o varios), tales como:

- Segmentación estricta y control de acceso (NAC/ACL/Firewall) + monitoreo reforzado SOC,
- Control de ejecución (allow□list) cuando aplique,
- Escaneo de archivos “en ruta” (servidores de escaneo) o arquitectura equivalente,
- Restricción de medios removibles y endurecimiento adicional, con evidencia y trazabilidad en ITSM.

S14.4. Despliegue por fases

S14.4.1. M1 — Alistamiento

- Inventario vs CMDB, brechas de cobertura.
- Diseño de políticas por perfil (endpoint/servidor Windows/servidor Linux/cloud/NAS).
- Integraciones SOC (SIEM/SOAR/ITSM/CMDB/Observabilidad) y fuentes XDR.
- Gobierno de contención (automático preaprobado / con aprobación / emergencia).
- Plan de despliegue por anillos (5%→20%→50%→100%) y rollback.

S14.4.2. Fase 1 — Piloto mínimo (medible)

- 10% endpoints (≈ 2.600).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- 10% servidores (≈ 60), mínimo 40 Linux y 20 Windows Server.
- XDR con correlación basada en ≥ 3 dominios adicionales a endpoint (p.ej., identidad + correo + SSE).
- Inicio de incorporación cloud (si existe) para telemetría y respuesta por fases.
- Implementación inicial NAS (al menos una sede) y plan de extensión a la segunda.

S14.4.3. Fase 2 — Despliegue por olas (cobertura total)
Despliegue progresivo hasta 26.000 endpoints y 500 servidores, por olas, con hiper-soporte, control de cambios ITIL y reversión.

S14.4.4. Fase 3 — Cloud workloads por fases
Incorporación progresiva de workloads cloud definidos por la ENTIDAD, garantizando equivalencia funcional y envío de eventos al SOC/XDR.

S14.5. Capacidades mínimas EPP/NGAV (Endpoints y Servidores)

S14.5.1. Prevención antimalware. Firmas/heurística + reputación + analítica/ML o equivalente verificable. Acciones: bloquear, limpiar, cuarentena, permitir con registro.

S14.5.2. Anti□ransomware. Detección por comportamiento y contención; rollback si la tecnología lo soporta o procedimientos de remediación integrados al SOC como servicio.

S14.5.3. Scripts/macros y abuso de herramientas. Controles configurables/auditables para PowerShell/WMI/JS/VBS/macros/persistencia (según OS y capacidades).

S14.5.4. Controles adicionales (cuando aplique). PUA/PUP, control de aplicaciones allow/deny, y/o integración con SSE para protección web.

S14.6. Capacidades mínimas tipo EDR Estas capacidades garantizan investigación y contención “mínima” en endpoint/servidor, independientemente del fabricante.

S14.6.1. Telemetría mínima.
- Árbol de procesos, hashes, usuario/sesión, eventos relevantes.
- Conexiones básicas (origen/destino/puerto) o equivalente.
- Persistencia relevante cuando aplique (servicios/tareas/startup).

S14.6.2. Contención mínima.
- Aislamiento lógico de red (o control equivalente) con excepciones controladas para comunicación con consola/SOC.
- Kill process, cuarentena, bloqueo IOC/hash.

S14.6.3. Recolección de artefactos.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Recolección remota de artefactos básicos (logs agente, procesos, muestras/archivos sospechosos, persistencia).
- Auditoría completa (quién/qué/cuándo) y vinculación al ticket ITSM.

S14.7. Capacidades XDR (Extended Detection & Response)

S14.7.1. Fuentes mínimas XDR (multi□dominio)

La plataforma XDR debe integrar, como mínimo (según existan en la ENTIDAD), estos dominios:

1. Endpoints/Servidores (EPP/EDR).
2. Identidad (AD on□premise y Entra ID o equivalente).
3. Correo/colaboración (M365 u otro).
4. SSE (SWG/CASB/ZTNA/DLP) cuando aplique.
5. Cloud (Azure y otros definidos) mediante logs/APIs soportadas.
6. Red (firewall perimetral y/o NDR si existe).
7. Threat Intelligence (IoCs).

S14.7.2. Correlación e incidente unificado

- Normalización, deduplicación y correlación en un incidente unificado con timeline y relaciones (host↔usuario↔correo↔IP/dominio↔recurso cloud).
- Severidad/prioridad configurables y ponderables por CMDB.
- Alertas/incidentes explicables (fuentes, evidencia, regla/modelo).

S14.7.3. Respuesta coordinada multi□dominio

Capacidad de ejecutar acciones (manual / con aprobación / automática preaprobada) en al menos:

- Endpoint/Server: aislamiento, cuarentena, bloqueo IOC/hash, recolección de artefactos.
- Identidad: revocar sesión/tokens, deshabilitar cuenta, forzar MFA/reset.
- Correo: cuarentena/purga, bloqueo remitente/URL/dominio.
- SSE: bloqueo dominio/URL, aislamiento de sesión/usuario, afinamiento de política (según aplique).
- Cloud: aislamiento workload, ajuste NSG/SG, revocación credenciales/llaves.

S14.7.4. La solución debe permitir, mediante mecanismos nativos o equivalentes, la recopilación y conservación de telemetría de endpoints y servidores, la trazabilidad de archivos, procesos, conexiones y eventos relevantes de seguridad, así como la reevaluación de indicadores o artefactos previamente observados cuando se actualice la inteligencia de amenazas.

S14.8. Gobernanza de contención, automatización y control de impacto

S14.8.1. Playbooks/runbooks con dos modalidades:

- Automática: solo escenarios preaprobados por la ENTIDAD.
- Con aprobación: para acciones de alto impacto (especialmente servidores críticos), registrando aprobación en ITSM institucional antes de ejecutar.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S14.8.2. "Acción de Emergencia" (solo críticos): si se define contractualmente, se permite contención urgente sin aprobación previa, registrándola en ITSM institucional en máximo 15 minutos con justificación y plan de reversión.

S14.8.3. Toda acción ejecutada debe quedar registrada con evidencia en ITSM institucional y bitácoras SOC/XDR.

S14.9. Integración con SOC/SIEM/SOAR/ITSM/CMDB

S14.9.1. SIEM/SOC. Envío de eventos/alertas/incidentes al SIEM del SOC como servicio (API/syslog/webhook o equivalente) con campos mínimos: activo, usuario, severidad, técnica/amenaza, acción, IOC/hash, timestamp, contexto CI/CMDB.

S14.9.2. SOAR. Disparadores para playbooks multi□dominio; human-in-the-loop según S9.13.2; evidencia en ITSM institucional.

S14.9.3. ITSM institucional (system of record). Tickets automáticos, actualización automática, sincronización de estados cuando aplique; idempotencia, colas/reintentos, trazabilidad de transacciones.

S14.9.4. CMDB. Enriquecimiento y priorización por criticidad/propietario/servicio/ambiente; inconsistencias CMDB reportadas como tickets de mejora.

S14.10. Protección Antimalware para NAS Hitachi HNAS Platform 4060 (Bogotá y Cali)

S14.10.1. Contexto de plataforma (provisto por la ENTIDAD)

- 2 soluciones HNAS (Bogotá y Cali).
- Cada solución: clúster físico con 2 nodos activos y un EVS lógico por nodo.
- Total: 4 nodos físicos y 4 EVS (los EVS son los que brindan servicio a usuarios).
- Carga estimada: 5.200–10.200 ops/s por nodo.
- Tamaño efectivo total: 120 TB Bogotá y 70 TB Cali.

Las referencias a Hitachi HNAS Platform 4060 corresponden exclusivamente a la identificación de los sistemas de almacenamiento existentes que deben ser protegidos y no constituyen una exigencia de marca respecto del motor o servicio antimalware ofertado.

S14.10.2. Método de integración (agentless) y compatibilidad HNAS

S14.10.2.1. La protección antimalware para HNAS debe operar en modalidad agentless, integrándose con Hitachi NAS Platform mediante mecanismos soportados para "virus scanning", incluyendo ICAP (o equivalente soportado por la versión instalada), agentes especializados, conectores nativos de almacenamiento, integraciones soportadas por fabricante o mecanismos técnicamente equivalentes, siempre que garanticen la cobertura efectiva de los repositorios definidos por la

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ENTIDAD, la detección de amenazas, la generación de alertas y las capacidades de respuesta requeridas en el Anexo Técnico.

S14.10.2.2. El PROVEEDOR debe proveer y configurar múltiples motores de escaneo (virus scan engines) para mejorar rendimiento y alta disponibilidad, según recomendación de la guía de Hitachi (múltiples engines para performance/HA).

S14.10.2.3. El PROVEEDOR debe dimensionar e implementar el número de motores, instancias o componentes de escaneo necesario para garantizar alta disponibilidad, capacidad, continuidad y ausencia de degradación material, con base en la carga medida y las recomendaciones soportadas de interoperabilidad del almacenamiento existente.

S14.10.2.4. La solución deberá garantizar la protección antimalware del contenido almacenado en los sistemas NAS mediante ICAP, agentes especializados, conectores nativos, servidores de escaneo, integración sobre recursos compartidos o mecanismos funcionalmente equivalentes oficialmente soportados.

La arquitectura deberá proporcionar análisis durante la escritura, incorporación o acceso cuando resulte técnicamente aplicable, así como escaneo programado y bajo demanda del contenido en reposo. El escaneo periódico no sustituirá la protección en tiempo cercano al real, salvo que se demuestre que los archivos no podrán ser accedidos, ejecutados o distribuidos antes de obtener un veredicto de seguridad.

Nota: La protección antimalware de las plataformas NAS deberá soportar, como mecanismo mínimo, la integración mediante el protocolo ICAP con las plataformas Hitachi HNAS. Adicionalmente, podrán utilizarse otros mecanismos soportados oficialmente por Hitachi y por el fabricante de la solución antimalware, siempre que garanticen análisis on-access, alta disponibilidad, rendimiento y trazabilidad hacia el SOC y el XDR, y se validen mediante documentación oficial y pruebas de aceptación. El escaneo bajo demanda o la inspección de tráfico en tránsito no sustituirán por sí solos el análisis on-access.

S14.10.3. Cobertura por sede, nodo y EVS

S14.10.3.1. El servicio debe proteger los 4 EVS (2 en Bogotá y 2 en Cali), garantizando operación consistente por EVS/share/export.

S14.10.4. Modos de escaneo

S14.10.4.1. On□access. Soportar escaneo on□access (lectura, escritura o ambas) parametrizable por EVS/share y documentado.

S14.10.4.2. On□demand/programado. Escaneo bajo demanda y programado por share/ruta lógica con reporte.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S14.10.4.3. Exclusiones y tamaño máximo. Permitir exclusiones y tamaño máximo de archivo bajo gobierno y auditoría (la guía HNAS contempla exclusiones y tamaño máximo de archivo para virus scanning).

S14.10.5. Dimensionamiento, desempeño y HA por sede

S14.10.5.1. El PROVEEDOR debe presentar un dimensionamiento por sede (Bogotá/Cali) que incluya:
- número de engines por sede (mínimo redundancia),
- concurrencia, colas y manejo de saturación,
- balanceo/failover,
- supuestos sobre modo on□access,
- reservas de crecimiento.

S14.10.5.2. El dimensionamiento debe considerar la carga estimada (5.200–10.200 ops/s por nodo) y demostrar, mediante medición en onboarding y pruebas, que el servicio de escaneo no introduce degradación material no controlada.

S14.10.5.3. Conectividad: el PROVEEDOR debe garantizar conectividad adecuada entre HNAS y servidores de escaneo; guías prácticas para integración con Hitachi NAS recomiendan enlaces de al menos 1 Gbps entre NAS y scan server para desempeño óptimo.

S14.10.5.4. La conectividad entre el almacenamiento y los componentes de escaneo deberá dimensionarse con base en la carga, concurrencia, tamaño de archivos, modalidad de escaneo y niveles de servicio exigidos, y validarse mediante pruebas de aceptación.

S14.10.6. Acciones mínimas y evidencia
- Denegar acceso, cuarentena, limpiar/eliminar (si aplica), con bitácora.
- Evidencia mínima: sede, EVS, share/ruta lógica, usuario/origen (si disponible), amenaza, acción, timestamp, motor/firma.

S14.10.7. Integración NAS con XDR/SOC
- Eventos NAS al SIEM.
- Correlación XDR con identidad/endpoints que acceden a shares para incidente unificado.
- Ticket ITSM vinculado al CI correcto (NAS y/o EVS).

S14.11. Operación, salud y postura

Monitoreo continuo de:
- Cobertura/health de agentes (26.000 endpoints, 500 servidores).
- Freshness de motor/firmas/modelos.
- Integraciones XDR (latencia, caídas, colas).
- NAS: salud de engines, colas ICAP, fallas y recuperación.

S14.12. Retención e integridad (alineada al SOC) — 36 meses

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S14.12.1. Retención mínima: 36 meses consultables y exportables de:

- Eventos/alertas/incidentes XDR, bitácoras, acciones, políticas y cambios.
- Eventos/acciones/evidencias de NAS.

S14.12.2. Integridad: preferible WORM/inmutabilidad o controles equivalentes verificables (hashing, segregación de funciones, auditoría).

S14.13. SLAs, KPIs y reportes (alineados al SOC)

S14.13.1. SLAs por severidad S1—S4 medidos en ITSM institucional.

S14.13.2. Reporte mensual mínimo:

- Cobertura/salud/freshness endpoints y servidores; brechas vs CMDB.
- Incidentes XDR correlacionados vs alertas; MTTD/MTTR y cumplimiento SLA.
- Acciones de respuesta por dominio y tasa de automatización.
- Excepciones/whitelists con expiración.
- NAS: volumen escaneos, detecciones, acciones, fallas/colas y conmutación.

S14.14. Pruebas de aceptación (criterios mínimos verificables)

S14.14.1. Piloto

Debe evidenciar:

1. Prevención/Detección: bloqueo/cuarentena de muestra controlada y escenario ransomware simulado.
2. EDR mínimo: telemetría + aislamiento + recolección artefactos con evidencia en ITSM institucional.
3. XDR real: al menos 1 incidente correlacionado con señales de ≥ 3 fuentes y timeline unificado; y ejecución controlada de ≥ 2 acciones en ≥ 2 dominios.
4. Integración SOC/ITSM/CMDB end□to□end.

S14.14.2. NAS (Bogotá y Cali)

En cada sede y validando cada EVS:

- On□access: archivo de prueba autorizado → detección y acción.
- On□demand: escaneo por share/ruta → reporte.
- SIEM + ticket ITSM con CI correcto.
- HA: falla controlada de un engine y continuidad del escaneo (múltiples engines para HA).

S14.14.3. Cobertura por OS

Pruebas representativas por familia (Windows/Windows Server/macOS/Linux). Para OS legacy sin agente, demostrar controles compensatorios y trazabilidad.

S14.15. Documentación técnica exigida

El PROVEEDOR deberá entregar al inicio del contrato:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		- Arquitectura EPP/NGAV+XDR (on□prem/nube/híbrida), HA/DR, RTO/RPO. - Plan por fases (piloto/olas/cloud) + despliegue por anillos + rollback. - Matriz de fuentes XDR e integraciones SOC/SIEM/SOAR/ITSM/CMDB. - Matriz de soporte OS/versión y controles compensatorios OS legacy. - Diseño y dimensionamiento NAS HNAS (ICAP, engines, HA, colas) por sede, considerando la carga estimada (ops/s) y capacidad (TB), con escalabilidad por tramos. - Runbooks/playbooks y gobernanza de contención. S14.16. Escalabilidad por tramos (control presupuestal) El OFERENTE debe ofertar tramos verificables para: - crecimiento de endpoints, servidores (Linux/Windows), y workloads cloud, - engines NAS por sede (capacidad/concurrencia/retención), - conectores XDR adicionales, evitando cláusulas ambiguas “sin costo adicional”. S14.17. Plan de salida (Exit Plan) Al finalizar el contrato, el PROVEEDOR debe entregar exportación completa de: - Inventario/cobertura histórica, - Eventos/alertas/incidentes/acciones (36 meses), - Políticas, excepciones y su historial, - Evidencias NAS y bitácoras asociadas, - Runbooks y documentación para transición, garantizando continuidad y auditabilidad.
	S15.	Servicio de Detección de Malware (Día Cero y APTs) — On-premise Y Nube — Integrado al SOC como Servicio S15.1. Objeto S15.1.1. El PROVEEDOR debe suministrar, implementar, operar y mantener un Servicio de Detección de Malware de Día Cero y APTs, capaz de identificar, analizar, clasificar, enriquecer y apoyar respuesta ante artefactos y actividades maliciosas (archivos, URLs, scripts, macros, binarios), en entornos on□premise, nube y/o híbridos, con integración al SOC como servicio 24x7. S15.1.2. El servicio debe soportar análisis estático y dinámico (sandboxing/detonación) en entornos aislados para entender comportamiento de artefactos desconocidos, técnica común para obtener evidencia adicional (comportamiento de red) y mejorar detección de día cero. S15.2. Alcance y cobertura mínima (on□premise, nube, híbrido) S15.2.1. Operación del servicio (asociado al SOC como servicio)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S15.2.1.1. El servicio debe operar bajo el modelo del SOC como servicio (L1/L2/L3 o equivalente), con reglas de escalamiento y trazabilidad en ITSM institucional, alineado con prácticas de gestión de incidentes y mejora continua.

S15.2.2. Cobertura de entornos

S15.2.2.1. On□premise: cobertura para análisis de artefactos originados en correo, navegación web, archivos compartidos, endpoints/servidores, y repositorios internos definidos.

S15.2.2.2. Nube/SaaS/IaaS: cobertura para artefactos y telemetría asociados a servicios cloud y SaaS definidos por la ENTIDAD (M365, aplicaciones SaaS, almacenamiento cloud), usando mecanismos soportados (APIs/logs).

S15.2.2.3. Híbrido: capacidad de correlación y trazabilidad entre señales on□premise y nube para detectar campañas APT (persistencia, movimiento lateral, C2, exfiltración) mapeadas a ATT&CK.

S15.3. Fuentes mínimas y canales de entrada (artefactos y señales)

S15.3.1. El PROVEEDOR debe habilitar recepción/análisis de artefactos desde, como mínimo:

- □ Correo y colaboración (adjuntos, URLs, payloads) y sus cuarentenas.
- □ Web/SSE (SWG/CASB) para descargas, URLs y cargas a SaaS según políticas.
- □ Endpoints/servidores (archivos sospechosos, scripts, eventos de ejecución) mediante integraciones con EDR/XDR/antimalware cuando existan.
- □ Repositorios on□premise y cloud (shares, almacenamiento cloud) para análisis bajo demanda y búsqueda de IoCs.
- □ Network artifacts (URL/DOMINIO/IP/hashes) provenientes del SOC/SIEM/NDR cuando existan para pivoteo de investigación.

S15.3.2. El servicio debe permitir APIs y conectores estándar (REST, webhook, syslog) para recepción de artefactos y envío de veredictos/IoCs, evitando dependencia de marca.

S15.4. Capacidades mínimas de análisis de malware (día cero y APT)

S15.4.1. Análisis estático

S15.4.1.1. El servicio debe realizar análisis estático que incluya, como mínimo:

- □ Extracción de hashes, firmas, metadatos, secciones, certificados, strings, macros, y IoCs (dominios/IP/URLs) cuando aplique.
- □ Clasificación por tipo de archivo (PE, scripts, documentos Office/PDF, archivos comprimidos) y detecciones heurísticas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S15.4.2. Análisis dinámico (sandbox/detonación)

S15.4.2.1. El servicio debe ejecutar artefactos en un entorno aislado (sandbox) para monitorear comportamiento en tiempo real (procesos, modificaciones de archivos, persistencia, tráfico de red) y generar reportes.

S15.4.2.2. El análisis dinámico debe incluir evidencia como:
- trazas de procesos, archivos creados/modificados, y comportamiento de red (idealmente con trazas/PCAP o evidencia equivalente), según la tecnología ofertada.

S15.4.2.3. El PROVEEDOR debe demostrar controles de aislamiento del sandbox (no propagación) y prácticas de diseño del entorno de análisis.

S15.4.3. Detección de técnicas APT y mapeo ATT&CK

S15.4.3.1. El servicio debe mapear hallazgos y comportamientos a tácticas/técnicas MITRE ATT&CK Enterprise y Cloud (cuando aplique), incluyendo al menos técnicas de: ejecución, persistencia, evasión, credenciales, movimiento lateral, C2, exfiltración e impacto.

S15.4.3.2. El reporte de análisis debe incluir el mapeo ATT&CK y evidencias que lo soporten.

S15.4.4. Anti-evasion y calidad de veredictos

S15.4.4.1. El servicio debe incluir mecanismos para aumentar efectividad frente a evasión (perfiles realistas, múltiples plantillas de SO, variación de entorno) y registrar si la muestra detecta sandbox/VM o falla ejecución.

S15.4.4.2. Los resultados del análisis deberán permitir clasificar las muestras, como mínimo, como maliciosas, benignas, sospechosas o de riesgo, e indeterminadas, pendientes o no concluyentes, aceptándose denominaciones funcionalmente equivalentes definidas por cada fabricante.

La solución debe proporcionar información técnica que permita sustentar y contextualizar el resultado obtenido, incluyendo, cuando aplique, nivel de riesgo, severidad, confianza, indicadores de compromiso, comportamientos observados, procesos, comunicaciones, artefactos, evidencias y acciones recomendadas.

No será obligatorio disponer de un puntaje numérico de confianza, siempre que la solución suministre un mecanismo equivalente, verificable y suficiente para interpretar el veredicto y definir las acciones de tratamiento.

El PROVEEDOR debe presentar una tabla de equivalencia entre las categorías utilizadas por su solución y las categorías funcionales requeridas por la ENTIDAD.

S15.5. Enriquecimiento, Threat Intel e IoCs

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S15.5.1. El servicio debe extraer, normalizar y gestionar IoCs (hashes, dominios, IPs, URLs) y permitir exportación en formatos estándar (STIX/TAXII o equivalentes) para su consumo por SIEM/SOAR/TIP si aplica.

S15.5.2. Debe soportar enriquecimiento con inteligencia de amenazas (fuentes internas/externas) y documentar periodicidad y trazabilidad de uso en casos.

S15.6. Integración con SOC (SIEM/SOAR/ITSM/CMDB)

S15.6.1. SIEM del SOC como servicio

S15.6.1.1. El servicio debe enviar eventos, veredictos, IoCs y evidencias al SIEM del SOC como servicio por mecanismos soportados (API/syslog/webhook), permitiendo correlación multi□fuente.

S15.6.1.2. Los eventos deben ser explicables y trazables (artefacto, fuente, técnica ATT&CK, score, evidencia).

S15.7. SOAR

S15.7.1.1. El servicio debe habilitar disparadores para playbooks SOAR, tales como:

- □ Bloqueo de URL/dominio/IP en SSE/FW,
- □ Cuarentena/purga de correo,
- □ Aislamiento de endpoint/host,
- □ Revocación de sesión de identidad, con gobernanza (automático preaprobado o con aprobación).

S15.7.2. ITSM institucional (system of record)

S15.7.2.1. Los incidentes/casos definidos por la ENTIDAD deben generar ticket en ITSM con: severidad/prioridad, evidencias, IoCs y acciones.

S15.7.2.2. La integración debe soportar idempotencia (no duplicación), reintentos/colas y trazabilidad de transacciones.

S15.7.3. CMDB

S15.7.3.1. Enriquecimiento de casos con criticidad del activo/servicio, propietario y metadatos, y vinculación del ticket al CI correspondiente.

S15.8. Desempeño, capacidad y niveles de servicio (SLA/SLO)

S15.8.1. Tiempos de análisis — mínimos exigibles. Los valores contractualmente vinculantes, su método de medición y las penalidades aplicables son los definidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S15.8.1.1. El PROVEEDOR debe cumplir los tiempos máximos para veredictos establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio, para los siguientes tipos de análisis:

- Estático, desde la recepción de la muestra (salvo colas).
- Dinámico/sandbox por muestra, incluyendo cola y ejecución, con prioridad para las muestras asociadas a incidentes de severidad S1 o S2 del SOC.
- Re-análisis/prioridad: colas “rush” para incidentes críticos del SOC.

S15.8.2. SLO de disponibilidad y colas

S15.8.2.1. Se exigirá el cumplimiento de los niveles de servicio establecidos en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio para:

- disponibilidad del servicio de análisis,
- entrega de veredictos y evidencias, con reporte de colas, fallas y tiempos de recuperación.

S15.8.3. Escalabilidad por tramos (control presupuestal)

S15.8.3.1. La escalabilidad debe ofertarse por tramos verificables: # muestras/día, # URLs/día, capacidad de sandbox concurrente, conectores, almacenamiento y retención, evitando “sin costo adicional” ambiguo.

S15.9. Retención, integridad, custodia y auditoría (alineado al SOC — 36 meses)

S15.9.1. Retención mínima

S15.9.1.1. El PROVEEDOR debe retener por mínimo 36 meses (consultable y exportable):

- veredictos, reportes de análisis (estático/dinámico), evidencias, IoCs, bitácoras, y trazabilidad de acciones.

S15.9.2. Integridad y protección de registros (preferible WORM/inmutabilidad)

S15.9.2.1. Los registros deben protegerse contra modificación/borrado no autorizado, con controles equivalentes a “protección de información de auditoría” y retención de registros (AU□9/AU□11 o equivalentes), preferiblemente con almacenamiento inmutable/WORM o medidas equivalentes verificables.

S15.10. Seguridad del servicio y privacidad

S15.10.1. Control de acceso con RBAC y MFA, segregación de funciones y auditoría de acciones administrativas/operativas.

S15.10.2. Cifrado en tránsito y reposo; segregación lógica (tenant/espacio dedicado o equivalente).

S15.10.3. Privacidad: minimización de exposición de datos (enmascaramiento/redacción) y cumplimiento del régimen aplicable de protección de datos personales.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S15.11. Entregables y reportes S15.11.1. Reporte mensual mínimo: - volumen de muestras/URLs analizadas, - top familias/campañas, - mapeo ATT&CK (técnicas más observadas), - falsos positivos/negativos y tuning, - salud de colas y disponibilidad, - mejoras realizadas y plan del mes siguiente. S15.11.2. Informe por incidente/caso: timeline, evidencia, IoCs, acciones ejecutadas, verificación y lecciones aprendidas. S15.12. Pruebas de aceptación Como condición de aceptación (por fases), el PROVEEDOR debe ejecutar y documentar: 1. Análisis estático: entrega de veredicto y extracción de IoCs sobre conjunto de muestras de prueba autorizadas. 2. Análisis dinámico/sandbox: detonación controlada de al menos 50 muestras/URLs con evidencia de comportamiento (procesos + red) y reporte completo. 3. Mapeo ATT&CK: reportes con técnicas/tácticas mapeadas y evidencia que las sustente (Enterprise y Cloud si aplica). 4. Integración SOC/ITSM/CMDB: creación automática de ticket ITSM, envío al SIEM y vinculación a CI/CMDB, con trazabilidad end□to□end. 5. Acción SOAR (si aplica): ejecución controlada de al menos 1 playbook (bloqueo URL/dominio o cuarentena correo) con aprobación cuando aplique. S15.13. Documentación técnica exigida El PROVEEDOR deberá entregar al inicio del contrato: - Arquitectura propuesta (on□prem/nube/híbrida) y controles de seguridad del sandbox. - Dimensionamiento (concurrencia sandbox, muestras/día, colas) y tramos de expansión. - Matriz de integraciones (SIEM/SOAR/ITSM/CMDB, M365/SSE/cloud) y plan de onboarding. - Evidencia de capacidades ATT&CK mapping y hunting. S15.14. Plan de salida (exit plan) Al finalizar el contrato, el PROVEEDOR debe entregar exportación completa de: - reportes, veredictos, IoCs, bitácoras y evidencias (36 meses), - configuración de políticas y conectores, - documentación/runbooks para transición, garantizando continuidad y auditabilidad.
S16.	SERVICIO DE SEGURIDAD EN LA NUBE — SASE (SECURITY ACCESS SERVICE EDGE) INTEGRADO CON SOC, ITSM Y OBSERVABILIDAD S16.1. Objeto, alcance y modalidad del servicio	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S16.1.1. EL PROVEEDOR debe suministrar, implementar, operar, monitorear y mantener un servicio administrado de seguridad en la nube bajo arquitectura SASE, orientado a proteger el acceso a Internet, el acceso a aplicaciones (en nube y on-premise) y el intercambio de datos de la ENTIDAD, conforme al diseño y fases aprobadas por la ENTIDAD. S16.1.2. EL PROVEEDOR debe asegurar que el servicio se integre con los componentes institucionales de operación de seguridad (SOC como servicio), la herramienta ITSM institucional (como "system of record"), la CMDB institucional (cuando aplique) y la herramienta de Observabilidad de la ENTIDAD. S16.1.3. EL PROVEEDOR debe suministrar licenciamiento para mínimo 1.000 usuarios con capacidad de aumentar a demanda de la ENTIDAD hasta 30.000 usuarios. S16.2. Arquitectura SASE y componentes mínimos S16.2.1. EL OFERENTE debe presentar la arquitectura SASE propuesta (puntos de presencia, flujos de tráfico, integración con SD-WAN, identidad y aplicaciones) para aprobación de la ENTIDAD, y ejecutarla sin afectar la continuidad del negocio. S16.2.2. EL PROVEEDOR debe proveer, como mínimo, capacidades de "Security Service Edge (SSE)" dentro del servicio SASE, habilitando controles de acceso y seguridad basados en identidad. S16.2.3. EL PROVEEDOR debe garantizar que el servicio soporte políticas basadas en identidad (usuario/grupo) e integración con el directorio/IdP institucional, para efectos de control y aplicación de políticas. S16.2.4. La solución debe proporcionar monitoreo de experiencia digital extremo a extremo mediante mediciones realizadas desde el dispositivo o contexto del usuario, los PoP del servicio, sondas sintéticas, telemetría de red e integraciones con las aplicaciones, según resulte aplicable. Debe permitir identificar el segmento probable de degradación entre el endpoint, red local, ISP, DNS, túnel o acceso seguro, PoP, tránsito y aplicación de destino. No se exigirá visibilidad literal sobre cada dispositivo intermedio de redes de terceros, siempre que la solución proporcione métricas y evidencias suficientes para determinar la causa probable y soportar la gestión del incidente. S16.3. Integración con SD-WAN y control basado en usuario S16.3.1. EL PROVEEDOR debe garantizar la interoperabilidad operativa entre SASE/SSE y el servicio SD-WAN, prestando los servicios de seguridad de manera local cuando el usuario esté conectado a la red corporativa, y haciéndolo mediante la inspección en plataforma SASE en Cloud cuando el usuario esté fuera de la red corporativa, habilitando políticas basadas en identidad que permitan

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

identificar flujos por usuario/grupo y aplicar controles conforme a lo definido por la ENTIDAD.

S16.3.2. EL PROVEEDOR debe soportar integración con mecanismos de autenticación usados en la administración de CPE (RADIUS/LDAP/TACACS+ cuando aplique), conforme al diseño aprobado por la ENTIDAD.

S16.4. Visibilidad, registros, eventos y reportes operacionales

S16.4.1. EL PROVEEDOR debe garantizar la generación de registros (logs) y eventos de seguridad del servicio SASE/SSE, incluyendo tráfico permitido y bloqueado, eventos de seguridad, y la generación de reportes operativos y ejecutivos.

S16.4.2. EL PROVEEDOR debe soportar la integración con el SIEM del SOC como servicio y con la herramienta de Observabilidad de la ENTIDAD, conforme a lo requerido por la ENTIDAD.

S16.5. Integración con SOC como servicio (SIEM/SOAR)

S16.5.1. (SIEM) EL PROVEEDOR debe enviar al SIEM del SOC como servicio los logs, eventos y alertas generados por el servicio SASE/SSE mediante mecanismos soportados (API/syslog/webhook o conectores estándar), garantizando continuidad de ingesta y disponibilidad de consulta.

S16.5.2. (SOAR) EL PROVEEDOR debe habilitar disparadores para playbooks SOAR relacionados con SASE/SSE (bloqueo de URL/dominio/IP, aislamiento de sesión, ajuste de políticas u otras acciones definidas por la ENTIDAD), bajo gobernanza definida (automático preaprobado o con aprobación).

S16.5.3. EL PROVEEDOR debe garantizar que los eventos enviados al SIEM sean explicables y trazables para correlación multi-fuente, conforme al modelo de operación del SOC.

S16.6. ITSM institucional (system of record, tickets automáticos y CMDB)

S16.6.1. EL PROVEEDOR debe integrar el servicio SASE/SSE con la herramienta ITSM institucional, de modo que todo incidente/caso y eventos correlacionados que la ENTIDAD defina generen automáticamente un ticket/caso en ITSM, incluyendo clasificación, severidad, prioridad, asignación, evidencias y trazabilidad.

S16.6.2. La integración ITSM debe soportar, como mínimo: (i) creación automática de tickets, (ii) actualización automática del ticket con estados/evidencias, (iii) sincronización de estados (bidireccional cuando el ITSM lo permita), (iv) trazabilidad completa de transacciones

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

(éxito/fallo/reintentos/latencia) e (v) idempotencia (no duplicación), incluyendo alertas por fallas de integración.

S16.6.3. La integración debe realizarse mediante mecanismos estándar soportados por el ITSM (APIs/servicios/webhooks o equivalentes), evitando requisitos direccionadores por marca.

S16.6.4. EL PROVEEDOR debe consumir la CMDB de la ENTIDAD para enriquecer eventos/alertas y tickets con criticidad, propietario, servicio relacionado, ambiente y metadatos del CI; y debe vincular cada ticket al CI correspondiente en CMDB para habilitar priorización automática y reportes por servicio/proceso.

S16.6.5. EL PROVEEDOR debe reportar inconsistencias CMDB (CI inexistente o atributos faltantes) como tickets de mejora/problema según el modelo ITSM de la ENTIDAD.

S16.6.6. Si la ENTIDAD migra de ITSM durante la ejecución, EL PROVEEDOR debe adaptar la integración al nuevo ITSM en el plazo máximo definido contractualmente, sin afectar la operación 24x7, y soportar operación paralela si la ENTIDAD lo exige.

S16.7. Integración con herramienta de Observabilidad de la ENTIDAD

S16.7.1. EL PROVEEDOR debe integrar el servicio SASE/SSE con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud del servicio, disponibilidad, estado de conectores/integraciones (SIEM/SOAR/ITSM cuando aplique), colas/reintentos cuando aplique y métricas operacionales agregadas (volumen de tráfico inspeccionado, permitido/bloqueado y eventos de seguridad), conforme defina la ENTIDAD.

S16.8. Implementación, transición, operación y mejora continua

S16.8.1. EL PROVEEDOR debe ejecutar la implementación por fases conforme al plan aprobado por la ENTIDAD, incluyendo instalación/configuración, pruebas, afinamiento de políticas y transición a operación.

S16.8.2. EL PROVEEDOR debe entregar documentación de arquitectura, configuración, operación y procedimientos (runbooks), y debe mantener evidencias de cambios (gestión de cambios) conforme al modelo de operación definido por la ENTIDAD.

S16.8.3. EL PROVEEDOR debe suministrar reportes operativos y ejecutivos periódicos, incluyendo tráfico permitido/bloqueado, eventos de seguridad y estado del servicio.

S16.9. Pruebas de aceptación (integraciones y operación)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S16.9.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencien como mínimo:

a) Operación del servicio SASE/SSE y aplicación de políticas basadas en identidad (usuario/grupo) según el diseño aprobado.
b) Evidencia de envío de logs/eventos al SIEM del SOC como servicio y su consulta/correlación básica.
c) Evidencia de disparadores/playbooks en SOAR, conforme a gobernanza definida por la ENTIDAD.
d) Evidencia de tickets automáticos en ITSM para los casos definidos por la ENTIDAD, con actualización y trazabilidad de transacciones, y vinculación a CI en CMDB cuando aplique.
e) Evidencia de visualización en Observabilidad de métricas/estado del servicio e integraciones (SIEM/SOAR/ITSM).

S16.9.2. EL PROVEEDOR debe consolidar los resultados de las pruebas de aceptación en un acta y un dossier de evidencias, conforme al procedimiento de aceptación definido por la ENTIDAD.

S16.10. Campos mínimos de eventos SASE para SIEM (SOC como servicio)

S16.10.1. EL PROVEEDOR debe garantizar que los logs, eventos y alertas generados por el servicio SASE/SSE y enviados al SIEM del SOC como servicio sean explicables y trazables, permitiendo su correlación multi-fuente.

S16.10.2. EL PROVEEDOR debe asegurar que el servicio SASE/SSE genere y envíe al SIEM, como mínimo, eventos asociados a: (i) tráfico permitido y bloqueado, (ii) eventos de seguridad, y (iii) reportes operativos/ejecutivos, conforme a los requerimientos del servicio y a la integración con SIEM definida por la ENTIDAD.

S16.10.3. Los eventos/alertas enviados al SIEM deben incluir, como mínimo, los siguientes campos (o su equivalente funcional en el formato del conector), sin perjuicio de campos adicionales del fabricante, y preservando la confidencialidad según políticas de la ENTIDAD:

a) timestamp (fecha/hora con zona horaria).
b) Source y categoría del control SASE/SSE que originó el evento.
c) PolicyId/RuleId y Action (permitir/bloquear/desafiar/aislar/forzar autenticación/poner en cuarentena/evitar descarga u otra acción equivalente).
d) Subject (usuario/grupo) cuando aplique, y contexto de identidad (IdP/SSO) cuando aplique.
e) Contexto de red (IP origen/destino, FQDN/URL, aplicación/categoría, puerto/protocolo) cuando aplique.
f) Severity/Criticality.

S16.11. Pruebas de aceptación para validación de campos mínimos en SIEM (SASE)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S16.11.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación orientadas a validar que los eventos/alertas del servicio SASE/SSE que se envían al SIEM del SOC como servicio cumplen con los campos mínimos definidos en S16.10 y que son explicables y trazables para correlación multi-fuente. S16.11.2. La ENTIDAD y EL PROVEEDOR deben validar, como mínimo, la recepción en el SIEM de eventos representativos de los principales controles/capacidades del servicio SASE/SSE (tráfico permitido/bloqueado y eventos de seguridad), conforme al diseño aprobado, verificando que para cada evento se registren los campos mínimos exigidos en S16.10.3. S16.11.3. Para la aceptación, EL PROVEEDOR debe aportar evidencias (capturas/exportaciones del SIEM y/o evidencias documentales del conector) demostrando que, para cada evento representativo validado, se encuentran presentes (o su equivalente funcional) como mínimo los campos listados en S16.10.3, incluyendo los campos de trazabilidad hacia SOAR/ITSM cuando aplique. S16.11.4. EL PROVEEDOR debe consolidar los resultados de estas pruebas en un acta de aceptación y un dossier de evidencias, dejando trazabilidad de los eventos validados, fuente de generación, mecanismo de integración hacia SIEM y resultado de verificación de campos mínimos definidos en S16.10.
	S17.	Servicio de Pruebas de Penetración S17.1. Objeto del servicio S17.1.1. El PROVEEDOR debe prestar el servicio de Pruebas de Penetración por campañas (Pentesting / Hacking Ético) que simule acciones de un atacante desde redes EXTERNAS e INTERNAS, conforme a una metodología reconocida como NIST SP 800-115 y/o PTES. S17.1.2. Para componentes de aplicaciones web y APIs, el PROVEEDOR debe aplicar OWASP WSTG, citando versión (estable/versionada) en planeación y reporte. S17.1.3. La severidad técnica de los hallazgos debe reportarse con CVSS v3.1 incluyendo vector. S17.2. Definiciones contractuales S17.2.1. EJECUCIÓN (Campaña): una campaña completa que incluye: a) prueba externa, b) prueba interna, c) informe ejecutivo + informe técnico (Informe Final), d) matriz de trazabilidad, e) un (1) re-test (validación de remediación) dentro de la misma ejecución. S17.2.2. Activo Objetivo: según aplique: aplicación web (FQDN/URL base), API (host + base path o colección), host/IP o

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

dispositivo/servicio de infraestructura, conforme matriz de alcance aprobada.

S17.3. Frecuencia mínima

S17.3.1. Durante la vigencia del contrato, el PROVEEDOR debe realizar como mínimo dos (2) por año.

S17.4. Alcance mínimo por EJECUCIÓN

S17.4.1. Cada EJECUCIÓN debe cubrir como mínimo diez (10) Activos Objetivo, definidos por la ENTIDAD, incluyendo aplicaciones web y APIs dentro de esos 10, además de infraestructura.

S17.4.2. La ENTIDAD y el PROVEEDOR aprobarán previo inicio una Matriz de Alcance que incluya: activos incluidos/excluidos, tipo (web/API/infra), ambiente, ventanas horarias y restricciones (rate limits).

S17.5. Modalidad de prueba

S17.5.1. La ENTIDAD definirá la modalidad por EJECUCIÓN: caja blanca, gris o negra.

S17.5.2. El PROVEEDOR debe advertir por escrito, antes de iniciar, las limitaciones de cobertura asociadas a la modalidad y los insumos mínimos requeridos.

S17.6. Acceso remoto y controles mínimos (SASE/SSE/Zero Trust)

S17.6.1. El acceso remoto se realizará únicamente mediante mecanismos autorizados por la ENTIDAD (VPN/ZTNA/bastión), con:
a) MFA obligatorio, b) cuentas nominativas, c) logging de accesos/actividad, d) ejecución en ventanas/horarios definidos por la ENTIDAD.

S17.6.2. El PROVEEDOR debe entregar y mantener actualizada la lista de IP(s) de egreso/origen para monitoreo/whitelisting institucional.

S17.7. Reglas de Compromiso (RoE)

S17.7.1. Previo a cada EJECUCIÓN, PROVEEDOR y ENTIDAD aprobarán el RoE, incluyendo:
a) alcance exacto, b) activos incluidos/excluidos, c) ventanas horarias, d) límites de tasa, e) exclusiones, f) procedimiento de “stop test”, g) canales de escalamiento/contactos, h) coordinación con mesa/SOC/CSIRT cuando aplique.

S17.7.2. Por defecto se prohíbe DoS/DDoS y pruebas de estrés, salvo autorización expresa por escrito en RoE.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S17.8. Exclusiones

S17.8.1. Se excluyen los ambientes/activos definidos por la ENTIDAD (producción crítica, forense, terceros), listados en la Matriz de Alcance.

S17.8.2. La ENTIDAD podrá definir ambientes equivalentes (staging/preproducción) o ventanas controladas para mantener cobertura.

S17.9. Entregables por EJECUCIÓN

S17.9.1. Por cada EJECUCIÓN el PROVEEDOR debe entregar como mínimo:
a) Informe Ejecutivo (postura general, riesgos principales y priorización).
b) Informe Técnico por hallazgo: descripción, evidencia, ruta de ataque, impacto, criticidad, recomendación, reproducibilidad, severidad CVSS v3.1 con vector, y resultado del re-test.
c) Matriz de trazabilidad (Activo ↔ Hallazgo ↔ Severidad ↔ Recomendación ↔ Estado ↔ Re-test).

S17.9.2. (Cuando aplique a web/APIs) referencia/mapeo a OWASP WSTG; y cuando la ENTIDAD lo solicite, mapeo a OWASP ASVS (versión definida).

S17.10. Notificación temprana

S17.10.1. Hallazgos Críticos confirmados deben notificarse por canal definido en RoE dentro de 24 horas desde su confirmación, sin esperar el informe final.

S17.11. Plazo de entrega del Informe Final

S17.11.1. El Informe Final (Informe Ejecutivo + Informe Técnico + Matriz de trazabilidad) debe entregarse dentro de diez (10) días hábiles contados a partir del cierre de pruebas de la EJECUCIÓN.

S17.11.2. El cierre de pruebas debe quedar documentado mediante acta/correo o mecanismo definido por la ENTIDAD.

S17.12. Re-test (validación de remediación)

S17.12.1. Cada EJECUCIÓN incluye un (1) re-test de validación de remediación, cuyos resultados deben quedar reflejados en el Informe Técnico y la Matriz de trazabilidad.

S17.13. No afectación del servicio / gestión de incidentes

S17.13.1. El PROVEEDOR debe minimizar el impacto operacional, ejecutar en coordinación con el Supervisor y acatar el RoE.

S17.13.2. Si ocurre una falla atribuible a la prueba, debe entregar informe de incidente con evidencias, línea de tiempo,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		actividades realizadas y detalle del servicio afectado, y apoyar el restablecimiento el tiempo requerido. S17.14. Idoneidad del personal S17.14.1. El servicio debe ser ejecutado por personal certificado en Penetration Testing/Ethical Hacking y experiencia comprobable. S17.14.2. El PROVEEDOR debe presentar hojas de vida y soportes con antelación a cada EJECUCIÓN y la ENTIDAD aprobará el recurso. S17.15. Manejo de información y evidencias S17.15.1. Evidencias y reportes deben protegerse con controles de confidencialidad y seguridad (cifrado, acceso restringido). S17.15.2. Se debe minimizar/anonimizar información sensible en evidencias cuando aplique, salvo autorización expresa en RoE.
	S18.	Servicio de Escaneo de Vulnerabilidades S18.1. Objeto del servicio S18.1.1. El PROVEEDOR debe prestar el servicio recurrente de escaneo, análisis, priorización, reporte, seguimiento y acompañamiento técnico para la gestión de vulnerabilidades sobre los activos tecnológicos definidos por la ENTIDAD, incluyendo direcciones IP privadas, activos on-premises y activos desplegados en nubes públicas o privadas, tales como Azure, Oracle Cloud Infrastructure, Google Cloud Platform u otras que la ENTIDAD determine. S18.1.2. El servicio debe permitir a la ENTIDAD identificar vulnerabilidades técnicas, debilidades de configuración, exposición innecesaria de servicios, riesgos asociados a sistemas operativos, bases de datos, aplicaciones, dispositivos de red, componentes de seguridad, plataformas cloud y demás activos incluidos en el alcance autorizado. S18.2. Alcance mínimo S18.2.1. El servicio cubrirá como mínimo dos mil (2.000) direcciones IP privadas o activos equivalentes definidos por la ENTIDAD, sin perjuicio de que la ENTIDAD pueda ajustar los rangos, segmentos, activos, sedes, zonas cloud o prioridades de evaluación durante la ejecución contractual, conforme a las necesidades institucionales. S18.2.2. El alcance debe incluir, como mínimo: a) Activos on-premises ubicados en centros de datos, sedes principales, sedes regionales o ambientes internos de la ENTIDAD. b) Activos desplegados en nubes públicas, privadas o híbridas, incluyendo máquinas virtuales, servicios expuestos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

internamente, subredes, balanceadores, contenedores, bases de datos, appliances virtuales y servicios administrados que permitan evaluación técnica.
c) Direcciones IP internas, rangos, segmentos, subredes, VLAN, zonas cloud, grupos de seguridad o equivalentes definidos por la ENTIDAD.
d) Activos críticos priorizados por la ENTIDAD, tales como servidores, plataformas misionales, servicios de autenticación, infraestructura de seguridad, componentes de red, sistemas de almacenamiento y servicios expuestos a otras redes internas o externas.
e) Activos nuevos que entren en operación durante la vigencia contractual, siempre que se encuentren dentro de la capacidad mínima contratada o de las condiciones de crecimiento pactadas.

S18.2.3. La ENTIDAD definirá los segmentos, rangos IP, cuentas cloud, suscripciones, compartimentos, proyectos, ventanas de ejecución y restricciones operativas. El PROVEEDOR debe documentar dicha información y mantener trazabilidad por ciclo de evaluación, incluyendo activos programados, activos efectivamente analizados, activos no alcanzados, exclusiones, causas de no evaluación y acciones requeridas para completar cobertura.

S18.3. Línea base, inventario y trazabilidad

El PROVEEDOR debe construir, mantener y actualizar una línea base del servicio, la cual debe contener como mínimo:
a) Identificador del activo o IP.
b) Segmento, subred, zona, suscripción, compartimento, proyecto cloud o ubicación lógica.
c) Tipo de activo, cuando sea identificable.
d) Sistema operativo o plataforma detectada, cuando aplique.
e) Criticidad del activo definida por la ENTIDAD.
f) Estado del activo frente al ciclo de escaneo: incluido, escaneado, no disponible, excluido, fallido o pendiente.
g) Fecha del último escaneo exitoso.
h) Fecha de la detección por primera vez.
i) Historial de vulnerabilidades críticas y altas.
j) Responsable funcional o técnico, cuando la ENTIDAD lo suministre.
k) Restricciones de escaneo, autenticación, ventana o exclusiones aplicables.

S18.3.1. La línea base debe ser entregada y actualizada mensualmente como parte de los entregables del servicio, en formato explotable definido por la ENTIDAD.

S18.4. Frecuencia mínima

S18.4.1. El PROVEEDOR debe realizar actividades de análisis de vulnerabilidad de manera mensual durante toda la vigencia del contrato (36 ciclos), salvo ajuste autorizado por escrito por la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.4.2. La frecuencia mensual constituye el mínimo exigible. La ENTIDAD podrá solicitar escaneos extraordinarios, reescaneos o validaciones puntuales sobre activos críticos, vulnerabilidades críticas, cambios relevantes de infraestructura, incidentes de seguridad, publicación de vulnerabilidades de alto impacto o necesidades institucionales, conforme a la bolsa de horas, capacidades incluidas o condiciones económicas pactadas.

S18.5. Plataforma(s), herramienta(s) o tecnología(s) utilizada(s)

S18.5.1. El PROVEEDOR debe disponer de herramientas especializadas para escaneo y análisis de vulnerabilidades, debidamente licenciadas, soportadas durante toda la vigencia contractual y de uso exclusivo para la prestación del servicio a la ENTIDAD.

S18.5.2. La solución utilizada debe permitir como mínimo:
a) Identificación de vulnerabilidades conocidas.
b) Clasificación por severidad.
c) Asociación con CVE, CVSS u otros identificadores técnicos reconocidos, cuando aplique.
d) Generación de reportes ejecutivos y técnicos.
e) Exportación en formatos explotables.
f) Priorización basada en criticidad técnica, criticidad del activo, exposición y contexto de riesgo.
g) Gestión histórica de hallazgos.
h) Comparación entre ciclos.
i) Reescaneo y validación de remediación.
j) Control de acceso a resultados.
k) Registro de evidencias y trazabilidad de ejecución.
l) Consulta mediante tableros (dashboards).

S18.5.3. El PROVEEDOR debe garantizar que las herramientas utilizadas se mantengan actualizadas en sus motores, firmas, plugins, catálogos de vulnerabilidades, plantillas, reglas y demás componentes requeridos para la correcta prestación del servicio.

S18.5.4. El PROVEEDOR debe suministrar accesos de consulta para las herramientas utilizadas en el servicio para los funcionarios que la ENTIDAD determine.

S18.6. Ejecución y coordinación

S18.6.1. Los escaneos deben ejecutarse exclusivamente en las ventanas autorizadas por la ENTIDAD, aplicando controles de tasa, concurrencia, intensidad, tiempos de espera, exclusiones y demás medidas necesarias para evitar afectación operacional.

S18.6.2. El PROVEEDOR debe coordinar con los responsables de infraestructura, seguridad, redes, nube, aplicaciones o áreas que la ENTIDAD determine para facilitar whitelist, credenciales o escaneos autenticados (si se autorizan).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.6.3. El PROVEEDOR debe contar con un procedimiento documentado de ejecución segura de escaneos, incluyendo criterios para pausar, suspender o ajustar la actividad ante degradación, alertas, indisponibilidad o riesgo operacional.

S18.7. Gestión de riesgos operacionales durante el escaneo

S18.7.1. El PROVEEDOR debe adoptar las medidas necesarias para minimizar el impacto de los escaneos sobre la disponibilidad, estabilidad, rendimiento, integridad y operación de los activos evaluados.
Como mínimo, debe:
a) Validar la ventana y alcance antes de cada ciclo.
b) Usar perfiles de escaneo acordes con la criticidad del ambiente.
c) Evitar pruebas destructivas, intrusivas o de explotación activa, salvo autorización expresa de la ENTIDAD.
d) Aplicar límites de concurrencia y tasa de conexión.
e) Suspender el escaneo si se identifica afectación operacional.
f) Informar oportunamente cualquier evento anómalo.
g) Documentar incidentes, ajustes y lecciones aprendidas.
h) Coordinar la reprogramación de activos no evaluados por causas de disponibilidad, restricción o riesgo.

S18.8. Criterios de severidad y priorización

S18.8.1. El PROVEEDOR debe clasificar los hallazgos con base en criterios técnicos reconocidos, incluyendo como mínimo severidad crítica, alta, media, baja e informativa.
La priorización debe considerar, como mínimo:
a) Severidad técnica de la vulnerabilidad.
b) CVSS o métrica equivalente.
c) Existencia de explotación conocida o pública.
d) Disponibilidad de exploit.
e) Exposición del activo.
f) Criticidad del activo definida por la ENTIDAD.
g) Componente afectado.
h) Antigüedad del hallazgo.
i) Reincidencia en ciclos anteriores.
j) Posible impacto sobre confidencialidad, integridad o disponibilidad.
k) Relación con amenazas activas, cuando la herramienta o fuentes de inteligencia lo permitan.

S18.8.2. El informe debe diferenciar claramente entre severidad técnica, riesgo contextual y prioridad de remediación.

S18.9. Validación de falsos positivos

S18.9.1. El PROVEEDOR debe realizar análisis y validación de falsos positivos para hallazgos críticos y altos cuando aplique, especialmente cuando el resultado pueda generar acciones operativas relevantes, cambios de configuración, ventanas de mantenimiento, aplicación de parches o decisiones de riesgo.
La validación debe incluir, como mínimo:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

a) Evidencia técnica del hallazgo.
b) Método de detección.
c) Condición que confirma o descarta la vulnerabilidad.
d) Limitaciones de validación, si existen.
e) Recomendación técnica.
f) Estado: confirmado, falso positivo, no concluyente, mitigado o pendiente de validación.

S18.10. Entregables por ciclo mensual

S18.10.1. Por cada ciclo mensual, el PROVEEDOR debe entregar un informe ejecutivo y un informe técnico que incluyan como mínimo:
a) Resumen ejecutivo del estado de vulnerabilidades.
b) Alcance programado y alcance efectivamente ejecutado.
c) Rangos IP, segmentos, activos, zonas cloud o grupos evaluados.
d) Activos excluidos, no disponibles, fallidos o no evaluados, con justificación.
e) Vulnerabilidades por severidad.
f) Vulnerabilidades por activo.
g) Vulnerabilidades por tecnología, sistema operativo, servicio o componente, cuando aplique.
h) Hallazgos críticos y altos con detalle técnico.
i) Recomendaciones de mitigación, parcheo, configuración o control compensatorio.
j) Tendencias frente a ciclos anteriores.
k) Hallazgos nuevos, persistentes, corregidos, reabiertos y recurrentes.
l) Validación de falsos positivos para hallazgos críticos y altos, cuando aplique.
m) Priorización de remediación.
n) Riesgos relevantes para la ENTIDAD.
o) Evidencias técnicas.
p) Conclusiones y acciones recomendadas.
q) Anexos en formatos explotables.

S18.10.2. El informe debe permitir diferenciar claramente entre hallazgos nuevos, hallazgos persistentes, hallazgos mitigados, hallazgos reabiertos y hallazgos aceptados por riesgo, si la ENTIDAD autoriza esta última condición.

S18.11. Formatos de entrega

S18.11.1. El PROVEEDOR debe entregar los informes y resultados en formatos explotables y reutilizables, incluyendo como mínimo:
a) PDF para informe ejecutivo y técnico.
b) XLSX o CSV para base de hallazgos.
c) JSON, XML u otro formato estructurado cuando la ENTIDAD lo requiera.
d) Evidencias técnicas anexas, cuando aplique.
e) Matriz de seguimiento de vulnerabilidades.
f) Matriz de activos cubiertos por ciclo.
g) Matriz de excepciones, exclusiones y activos no evaluados.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.11.2. Los archivos deben estar organizados por ciclo, fecha, alcance y versión, garantizando trazabilidad y facilidad de consulta.

S18.12. Acompañamiento técnico

S18.12.1. El PROVEEDOR debe realizar acompañamiento técnico para la mitigación de vulnerabilidades, conforme al alcance contractual y los requerimientos establecidos en las fichas técnicas.

S18.12.2. El acompañamiento debe incluir, como mínimo:
a) Explicación técnica de vulnerabilidades detectadas con severidad crítica y alta, así como posibles riesgos asociados.
b) Recomendaciones de remediación y mitigación.
c) Recomendaciones de controles complementarios ante escenarios donde las acciones de remediación y mitigación recomendadas no sean viables.
d) Coordinación y acompañamiento en sesiones técnicas con responsables y actores identificados en la remediación y mitigación de las vulnerabilidades detectadas y reportadas dentro de la ejecución del contrato o por la ENTIDAD.
e) Definición de la priorización de acciones a realizar con los responsables y administradores de las plataformas vulnerables.
f) Revisión de avances y evidencias de la ejecución de las acciones de remediación y mitigación.
g) Reescaneo o validación posterior a la corrección o solicitud de la ENTIDAD.
h) Documentación de acciones realizadas y estado final.
i) Formulación y determinación de planes que incluyan cronogramas de mitigación y remediación de las vulnerabilidades detectadas estableciendo actividades, responsables, actores (administradores y especialistas en las plataformas relacionadas), recursos y tiempos de ejecución.

S18.12.3. El PROVEEDOR debe realizar la coordinación y seguimiento de la ejecución de actividades correspondientes a la administración directa de infraestructura que presenta vulnerabilidades detectadas, así como cambios productivos, aplicación de parches o modificación de configuraciones.

S18.13. Integración con herramientas institucionales

S18.13.1. El PROVEEDOR debe enviar los resultados de los análisis de vulnerabilidades a las plataformas SIEM y SOAR del SOC como servicio.

S18.14. Seguridad de la información y confidencialidad

S18.14.1. El PROVEEDOR debe proteger toda la información obtenida, generada o tratada durante la prestación del servicio, incluyendo inventarios, direcciones IP, vulnerabilidades, evidencias, configuraciones, credenciales, reportes, topologías, diagramas, resultados técnicos y cualquier otra información sensible de la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.14.2. El PROVEEDOR debe cumplir, como mínimo, con las siguientes obligaciones:

a) Mantener confidencialidad sobre la información tratada y suscribir los acuerdos de confidencialidad del caso mediante los formatos establecidos por la ENTIDAD.
b) Usar la información exclusivamente para la prestación del servicio.
c) Proteger reportes y bases de datos mediante mecanismos seguros.
d) No divulgar información a terceros sin autorización de la ENTIDAD.
e) Notificar cualquier incidente de seguridad asociado al servicio.
f) Eliminar, devolver o transferir la información al finalizar el contrato, según instrucción de la ENTIDAD.
g) Garantizar que el personal asignado conozca y cumpla las obligaciones de confidencialidad.

S18.15. Gestión de excepciones

S18.15.1. El PROVEEDOR debe documentar las vulnerabilidades que no puedan ser mitigadas por restricciones técnicas, dependencia de fabricante, obsolescencia, indisponibilidad de parche, riesgo operacional o decisión de la ENTIDAD.

S18.15.2. La matriz de excepciones debe incluir como mínimo:

a) Vulnerabilidad.
b) Activo afectado.
c) Severidad.
d) Justificación.
e) Riesgo asociado.
f) Control compensatorio recomendado.
g) Responsable de decisión.
h) Fecha de autorización.
i) Vigencia de la excepción.
j) Fecha de revisión.
k) Aprobación por parte del dueño o responsable del activo.

S18.16. Gestión de vulnerabilidades críticas o de alto impacto

S18.16.1. Cuando se identifiquen vulnerabilidades críticas, altas o de explotación activa conocida, el PROVEEDOR debe generar una notificación prioritaria a la ENTIDAD, sin esperar la entrega del informe mensual completo.

S18.16.2. La notificación debe incluir como mínimo:

a) Identificación del activo.
b) Descripción de la vulnerabilidad.
c) Severidad.
d) Evidencia técnica.
e) Impacto potencial.
f) Recomendación de mitigación inmediata.
g) Recomendación de control complementario, cuando aplique.
h) Necesidad de reescaneo o validación.

S18.17. Reportes y formatos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.17.1. El PROVEEDOR debe entregar los informes y resultados en formatos explotables (PDF + CSV/XLSX/JSON u otro que defina la ENTIDAD) para facilitar análisis y seguimiento.

S18.17.2. No se aceptarán reportes que contengan únicamente salidas automáticas de herramienta sin análisis técnico, priorización, contexto, recomendaciones o depuración mínima de resultados.

S18.17.3. El PROVEEDOR debe entregar los informes mensuales del servicio durante los primeros cinco (5) días del mes siguiente.

S18.18. Gobierno del servicio

S18.18.1. El PROVEEDOR debe coordinar reuniones periódicas de seguimiento con la ENTIDAD, con la frecuencia definida contractualmente.

S18.18.2. En dichas reuniones se revisará como mínimo:
a) Estado del ciclo mensual.
b) Cobertura alcanzada.
c) Hallazgos críticos y altos.
d) Tendencias.
e) Vulnerabilidades recurrentes.
f) Activos no evaluados.
g) Acciones de mitigación.
h) Reescaneos.
i) Riesgos y bloqueantes.
j) Cumplimiento de ANS.
k) Oportunidades de mejora.

S18.18.3. El PROVEEDOR debe elaborar actas, compromisos o matrices de seguimiento cuando la ENTIDAD lo solicite.

S18.19. Indicadores mínimos del servicio

S18.19.1. El PROVEEDOR debe entregar indicadores mensuales que permitan medir evolución, cobertura y efectividad del servicio. Como mínimo:
a) Porcentaje de activos evaluados frente al alcance programado.
b) Número de vulnerabilidades por severidad.
c) Número de vulnerabilidades nuevas.
d) Número de vulnerabilidades mitigadas.
e) Número de vulnerabilidades persistentes.
f) Número de vulnerabilidades reabiertas.
g) Edad promedio de vulnerabilidades críticas y altas.
h) Activos con mayor concentración de riesgo.
i) Tecnologías con mayor recurrencia de hallazgos.
j) Cumplimiento de ANS.
k) Reescaneos ejecutados.
l) Falsos positivos identificados.

S18.20. Condiciones para ambientes cloud

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S18.20.1. Para activos desplegados en Azure, Oracle Cloud, Google Cloud u otras nubes, el PROVEEDOR debe considerar las restricciones técnicas, contractuales y de seguridad propias de cada plataforma.

S18.20.2. El PROVEEDOR debe coordinar con la ENTIDAD, antes de cualquier evaluación cloud:
a) Alcance autorizado.
b) Cuentas, suscripciones, compartimentos, proyectos o redes involucradas.
c) Activos permitidos.
d) Métodos de evaluación autorizados.
e) Restricciones del proveedor cloud.
f) Reglas de seguridad y alertamiento en nubes.
g) Ventanas de ejecución.
h) Mecanismos de autenticación.
i) Exclusiones técnicas.
j) Evidencias permitidas.

S18.20.3. El PROVEEDOR no podrá realizar pruebas intrusivas, explotación, denegación de servicio, pruebas destructivas o actividades no permitidas por la ENTIDAD o por las condiciones del proveedor cloud.

S18.21. Requisitos de transición de entrada del servicio

S18.21.1. Al inicio del contrato, el PROVEEDOR debe ejecutar una fase de alistamiento o transición del servicio con respecto al contrato, que incluya como mínimo:
a) Reunión de inicio.
b) Recolección de información de alcance.
c) Identificación de responsables.
d) Definición de ventanas de escaneo.
e) Definición de formatos de reporte.
f) Definición de criterios de severidad y priorización.
g) Parametrización o despliegue de herramientas.
h) Validación de conectividad.
i) Prueba controlada de escaneo sobre muestra autorizada.
j) Ajuste de perfiles de escaneo.
k) Elaboración del plan mensual de ciclos.
l) Entrega del plan de trabajo del servicio.

S18.22. Plan de salida, reversibilidad y transferencia

S18.22.1. El PROVEEDOR debe presentar, mantener actualizado y ejecutar un plan de salida o terminación del servicio, con el fin de asegurar la continuidad operativa, la transferencia ordenada de información y la reversibilidad del servicio al finalizar el contrato, por terminación normal, terminación anticipada, cesión, suspensión o cambio de proveedor.

S18.22.2. El plan de salida debe incluir como mínimo:
a) Inventario final de activos incluidos en el servicio.
b) Histórico de escaneos ejecutados y de informes presentados.
c) Histórico de vulnerabilidades por activo y severidad.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

d) Estado final de vulnerabilidades: abiertas, mitigadas, persistentes, reabiertas, aceptadas por riesgo o excluidas.
e) Matriz de hallazgos críticos y altos vigentes.
f) Matriz de excepciones y aceptaciones de riesgo autorizadas por la ENTIDAD.
g) Reportes finales en PDF y formatos explotables.
h) Entrega de bases de datos, exportaciones, evidencias y anexos generados durante el contrato.
i) Documentación de configuración del servicio, perfiles de escaneo, criterios de priorización y plantillas de reporte.
j) Procedimiento de desinstalación o retiro de agentes, appliances, conectores o componentes instalados, si aplica.
k) Eliminación segura de información en poder del PROVEEDOR, cuando así lo indique la ENTIDAD.
l) Certificación de devolución, transferencia o eliminación de información.
m) Entrega de lecciones aprendidas y recomendaciones de continuidad.
o) Acta de cierre técnico del servicio.

S18.22.3. El PROVEEDOR debe garantizar que la salida del servicio no implique pérdida de información histórica, dependencia tecnológica injustificada, bloqueo de acceso a reportes, retención no autorizada de información o interrupción en la capacidad de seguimiento de vulnerabilidades de la ENTIDAD.

S18.23. Propiedad de la información

S18.23.1. Toda la información generada, recolectada o procesada durante la prestación del servicio será propiedad de la ENTIDAD, incluyendo reportes, matrices, evidencias, históricos, configuraciones documentadas, exportaciones, indicadores, planes, actas y demás entregables.

S18.23.2. El PROVEEDOR no podrá retener, reutilizar, comercializar, divulgar o transferir dicha información sin autorización previa y expresa de la ENTIDAD.

S18.24. Cierre mensual y cierre contractual

S18.24.1. Cada ciclo mensual debe cerrarse mediante entrega formal de reportes, matriz de hallazgos, evidencias, indicadores y, cuando aplique, acta o correo de cierre del ciclo.

S18.24.2. Al finalizar el contrato, el PROVEEDOR debe entregar un informe consolidado de cierre contractual que incluya:
a) Resumen ciclos ejecutados durante la ejecución del contrato.
b) Evolución de vulnerabilidades.
c) Principales riesgos identificados.
d) Vulnerabilidades críticas y altas pendientes.
e) Activos con mayor exposición.
f) Recomendaciones estratégicas.
g) Estado de cumplimiento de ANS.
h) Ejecución del plan de salida.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		i) Certificación de entrega o eliminación de información. j) Relación de pendientes y recomendaciones para continuidad.
	S19.	Servicio de Pruebas de Penetración Persistente S19.1. OBJETO DEL SERVICIO S19.1.1. El PROVEEDOR debe prestar un servicio de Pruebas de Penetración Persistente orientado a explotación controlada, que simule acciones de un atacante real de forma continua, con el fin de: a) identificar rutas de ataque explotables (cadenas de vulnerabilidades), b) validar impacto real (técnico y operacional), c) evaluar exposición/detección/respuesta (si aplica), d) soportar la priorización de remediación y verificación de cierre. S19.1.2. El servicio debe ejecutarse conforme a metodologías reconocidas para pruebas de seguridad técnica, tales como NIST SP 800-115 y/o PTES, con un proceso formal de planeación, ejecución, evidencias y reporte. S19.1.3. Los hallazgos deben calificarse con severidad técnica usando CVSS v3.1 incluyendo vector. S19.2. DEFINICIONES S19.2.1. Pentesting Persistente (Explotación): ejecución continua y reiterada de actividades ofensivas con validación por explotación controlada, limitada por RoE, cuyo propósito es demostrar si un atacante pudiese comprometer activos definidos. S19.2.2. Ventana de explotación: periodo(s) autorizado(s) en el cual se permite explotación controlada (por defecto restringida y con límites). S19.2.3. Persistencia (permitida/restringida): mantenimiento controlado de acceso para validación y evidencia, con restricciones explícitas (ver numeral S19.8). S19.2.4. Activos Objetivo: dominios, subdominios, aplicaciones web/APIs, IP públicas/privadas, servicios y/o segmentos definidos en Matriz de Alcance. S19.3. ALCANCE MÍNIMO Y COBERTURA S19.3.1. La ENTIDAD definirá el alcance exacto en una Matriz de Alcance que contenga, como mínimo: a) dominios/URL base, APIs, IPs/segmentos, servicios y ambientes incluidos, b) activos excluidos, c) ventanas horarias y límites de tasa, d) clasificación de criticidad del activo. S19.3.2. El servicio debe operar en modalidad continuada durante la vigencia del contrato, con actividades 7x24, salvo las

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

restricciones de ventana de explotación y/o activos críticos definidas por la ENTIDAD en RoE.

S19.3.3. El PROVEEDOR debe proponer un modelo de cobertura mínimo, que incluya:
a) frecuencia de intentos de validación/explotación por categoría de activo,
b) criterios para escalamiento (pasar de hallazgo a explotación controlada),
c) manejo de falsos positivos (validación).

S19.4. MODALIDAD Y PERFIL DE ADVERSARIO

S19.4.1. La ENTIDAD definirá el tipo de ejercicio por periodo: caja negra, gris o blanca, y el "perfil adversario" (nivel de sigilo/ruido, alcance de credenciales, etc.), el cual se reflejará en el RoE.

S19.4.2. El PROVEEDOR debe advertir por escrito las limitaciones de cobertura asociadas a la modalidad y requerimientos mínimos (credenciales, bastiones, acceso, información técnica).

S19.5. REGLAS DE COMPROMISO (RoE)

S19.5.1. Antes de iniciar el servicio (y antes de cada cambio mayor), se debe aprobar un RoE que incluya como mínimo:
a) activos incluidos/excluidos,
b) ventanas de operación y ventanas específicas de explotación,
c) límites de tasa (rate limits),
d) prohibiciones explícitas (por defecto no DoS/DDoS),
e) "stop test / kill switch" y criterios de activación,
f) canales de escalamiento 7x24 (técnico y directivo),
g) protocolo de notificación de hallazgos críticos,
h) coordinación con SOC/CSIRT (si aplica),
i) lineamientos de manejo de evidencias.

S19.5.2. Por defecto, se prohíbe cualquier prueba de disponibilidad (DoS/DDoS), salvo autorización expresa por escrito en RoE.

S19.6. ACCESO REMOTO Y CONTROLES MÍNIMOS (ZERO TRUST)

S19.6.1. El acceso del PROVEEDOR será únicamente mediante mecanismos autorizados por la ENTIDAD (VPN/ZTNA/bastión), con:
a) MFA obligatorio,
b) cuentas nominativas (no compartidas),
c) registro (logging) de accesos y actividad,
d) ejecución en horarios/ventanas definidos por la ENTIDAD, especialmente para explotación.

S19.6.2. El PROVEEDOR debe suministrar y mantener actualizada la lista de IP(s) de egreso/origen y huellas necesarias para monitoreo institucional.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S19.7. CONTROLES DE SEGURIDAD OPERACIONAL (NO AFECTACIÓN)

S19.7.1. El PROVEEDOR debe minimizar el impacto operacional y ejecutar con límites de seguridad. Debe incluir medidas como:
a) límites de concurrencia y tasa,
b) pruebas escalonadas (de baja a mayor intrusión),
c) coordinación previa para pruebas en activos sensibles.

S19.7.2. En caso de afectación atribuible a la prueba:
a) activar procedimiento de "stop test",
b) emitir informe de incidente con evidencias y línea de tiempo,
c) apoyar restablecimiento del servicio hasta su normalización.

S19.8. RESTRICCIONES ESPECÍFICAS PARA "EXPLOTACIÓN" Y "PERSISTENCIA"

S19.8.1. Explotación controlada: solo se permitirá dentro de las ventanas autorizadas y bajo los límites del RoE.

S19.8.2. Persistencia permitida (si la ENTIDAD la autoriza):
a) solo para demostrar impacto y/o ruta de ataque,
b) con mecanismos temporales, trazables y removibles,
c) prohibido instalar software no autorizado o alterar configuraciones permanentes.

S19.8.3. Prohibiciones mínimas (salvo autorización expresa por escrito):
a) exfiltración de datos reales (solo evidencias mínimas/anonimizadas),
b) movimiento lateral hacia activos fuera de alcance,
c) uso de técnicas destructivas, cifrado, wipers o acciones irreversibles,
d) creación de cuentas persistentes no aprobadas,
e) alteración de registros o borrado de evidencias.

S19.8.4. Criterio de evidencia: se debe demostrar impacto con evidencias no sensibles, o con muestras mínimas definidas por la ENTIDAD.

S19.9. GESTIÓN CONTINUA, SEGUIMIENTO Y CICLO DE VIDA DE HALLAZGOS

S19.9.1. El PROVEEDOR debe operar un flujo continuo: Detección → Validación → Explotación controlada (si aplica) → Reporte → Remediación → Re-validación.

S19.9.2. El PROVEEDOR debe mantener una matriz de trazabilidad viva: Activo ↔ Hallazgo ↔ Severidad ↔ Evidencia ↔ Estado ↔ Responsable ↔ Fechas ↔ Revalidación.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S19.9.3. El PROVEEDOR debe proporcionar acompañamiento técnico para mitigación (con alcance definido: incluido o bolsa de horas).

S19.10. ENTREGABLES Y REPORTERÍA

S19.10.1. Notificación inmediata: hallazgos críticos explotables deben notificarse en un máximo de 24 horas desde su confirmación.

S19.10.2. Reporte periódico:

a) Informe semanal operativo: nuevos hallazgos, explotaciones realizadas (si aplican), cambios de estado, riesgos emergentes.
b) Informe mensual ejecutivo: tendencias, top riesgos, activos más expuestos, recomendaciones priorizadas.

S19.10.3. Informe técnico por hallazgo (cada hallazgo confirmado):
descripción, evidencia, ruta de ataque (a nivel de narrativa y condiciones, sin exponer datos sensibles), impacto, criticidad, recomendación, CVSS v3.1 con vector.

S19.10.4. Revalidación: el PROVEEDOR debe revalidar hallazgos remediados e informar el estado (cerrado/no cerrado) en la matriz.

S19.11. PLATAFORMA DE GESTIÓN

S19.11.1. El PROVEEDOR debe proveer una plataforma (o módulo) para que la FGN pueda:
a) ver activos monitoreados, hallazgos, evidencias, historial, y estados,
b) asignar responsables, fechas objetivo y comentarios,
c) exportar reportes/datasets en formatos explotables (PDF/CSV/JSON),
d) configurar notificaciones (por severidad/activo/regla).

S19.11.2. La plataforma debe soportar roles, auditoría de accesos y MFA.

S19.12. IDONEIDAD DEL PERSONAL Y DISPONIBILIDAD (OPERACIÓN 7x24)

S19.12.1. El servicio debe ser ejecutado por personal certificado y con experiencia comprobable; el PROVEEDOR debe presentar hojas de vida y soportes para aprobación de la ENTIDAD.

S19.12.2. El PROVEEDOR debe garantizar un esquema 7x24 de atención/escala para:
a) notificación de críticos,
b) activación de stop test,
c) coordinación ante incidentes.

S19.13. CONFIDENCIALIDAD, MANEJO DE DATOS Y EVIDENCIAS

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S19.13.1. El PROVEEDOR debe aplicar controles de confidencialidad: cifrado de evidencias, control de acceso, y retención/borrado conforme lineamientos de la ENTIDAD. S19.13.2. Evidencias deben minimizar datos sensibles y evitar exposición de información misional; cualquier excepción debe autorizarse por escrito. S19.14. CRITERIOS DE ACEPTACIÓN (VERIFICABILIDAD) S19.14.1. El servicio se aceptará contra evidencias mínimas: a) RoE aprobado y vigente, b) matriz de alcance y trazabilidad actualizada, c) notificaciones de críticos dentro del SLA, d) reportes semanales/mensuales entregados, e) informes técnicos con CVSS v3.1 + vector, f) registro de actividades (bitácoras) y control de cambios. S19.15. DIFERENCIACIÓN RESPECTO A ASM S19.15.1. Este servicio (Pentesting Persistente de explotación) NO es equivalente a ASM discovery 24/7: ASM se centra en descubrimiento y exposición (identificar/alertar). Este servicio incorpora explotación controlada y eventualmente persistencia autorizada para demostrar impacto.
	S20.	Servicio PAM (Privileged Access Management) Integrado con SOC, ITSM y Observabilidad *El servicio será operado por los perfiles descritos en el Anexo Técnico 6 — Perfiles Profesionales, numeral P3 (Perfiles técnicos de Seguridad).* S20.1. Objeto y alcance S20.1.1. EL PROVEEDOR debe suministrar, implementar, operar y mantener un servicio PAM (Privileged Access Management) para controlar, auditar y asegurar el acceso privilegiado a activos y sistemas de la ENTIDAD, incluyendo cuentas privilegiadas, sesiones, secretos y flujos de aprobación, conforme a los casos de uso definidos por la ENTIDAD. S20.1.2. EL PROVEEDOR debe garantizar que el servicio PAM se integre con el SOC como servicio (SIEM/SOAR), utilice la herramienta ITSM institucional como “system of record” (con CMDB cuando aplique) y se integre con la herramienta de Observabilidad de la ENTIDAD. S20.2. Alcance y capacidades (gestión de credenciales y secretos) S20.2.1. Bóveda de contraseñas (Vaulting): EL PROVEEDOR debe proveer capacidad de custodiar, proteger y administrar credenciales privilegiadas mediante una bóveda segura, repositorio controlado soportado por la solución.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S20.2.2. Rotación automática: EL PROVEEDOR debe proveer capacidad de rotación, actualización, expiración, revocación o renovación controlada de credenciales privilegiadas, conforme a políticas definidas por la ENTIDAD.

S20.2.3. Descubrimiento de cuentas: EL PROVEEDOR debe habilitar escaneo/descubrimiento automatizado para identificar cuentas privilegiadas “olvidadas” o no inventariadas, y permitir su incorporación a la bóveda y a las políticas.

S20.2.4. Autenticación reforzada: EL PROVEEDOR debe integrar el PAM con mecanismos de autenticación reforzada, incluyendo cuando aplique MFA, SSO o controles equivalentes, conforme al modelo de identidad de la ENTIDAD.

S20.2.5. Gestión de secretos: EL PROVEEDOR debe habilitar integración con aplicaciones, scripts o automatizaciones para eliminar contraseñas “hardcodeadas”, gestionando secretos de forma centralizada y controlada.

S20.2.6. Préstamo controlado de credenciales: EL PROVEEDOR debe habilitar préstamo controlado (check-in/check-out), credenciales temporales, acceso bajo demanda u otros mecanismos equivalentes, con trazabilidad y vencimiento según políticas.

S20.3. Gestión de sesiones y auditoría

S20.3.1. Aislamiento de sesiones (Proxy/Jump): EL PROVEEDOR debe garantizar aislamiento de sesiones privilegiadas, estableciendo el acceso a través de un salto (jump server) o proxy gestionado por el PAM, aprobado por la ENTIDAD.

S20.3.2. Grabación de sesiones: EL PROVEEDOR debe monitorear y registrar sesiones privilegiadas, incluyendo evidencia técnica; y debe soportar registro en video y texto (logs de comandos) para sesiones RDP, SSH o web.

S20.3.3. Monitoreo en tiempo real: EL PROVEEDOR debe permitir que un supervisor visualice la sesión en vivo y pueda finalizarla ante actividad sospechosa, dejando trazabilidad de la acción.

S20.3.4. Búsqueda por comandos: EL PROVEEDOR debe permitir búsqueda dentro de grabaciones para identificar cuándo se ejecutó un comando específico (comandos destructivos o de administración).

S20.4. Control de acceso y políticas (ZSP/JIT/PoLP)

S20.4.1. Zero Standing Privilege (ZSP): EL PROVEEDOR debe proporcionar capacidades de Zero Standing Privilege (ZSP) o equivalente, reduciendo privilegios permanentes y habilitando acceso privilegiado solo cuando sea requerido.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S20.4.2. Acceso Just-In-Time (JIT): EL PROVEEDOR debe soportar acceso privilegiado Just-In-Time (JIT) conforme a perfiles/eventos/casos de uso definidos por la ENTIDAD.

S20.4.3. Flujos de aprobación: EL PROVEEDOR debe habilitar flujos de aprobación previos a la liberación de credenciales y/o habilitación de sesión, requiriendo aprobación de supervisor cuando así lo defina la ENTIDAD.

S20.4.4. MFA para portal PAM y accesos: EL PROVEEDOR debe exigir MFA (u otro control equivalente) para ingresar al portal PAM y para operaciones privilegiadas definidas por la ENTIDAD, integrado al esquema de identidad/SSO cuando aplique.

S20.4.5. Principio de menor privilegio: EL PROVEEDOR debe habilitar elevación de privilegios solo para tareas específicas (task-based elevation), evitando conceder acceso total de root/administrador cuando no sea necesario.

S20.4.6. Control de acceso privilegiado por criterios: EL PROVEEDOR debe aplicar políticas de acceso privilegiado basadas en roles, atributos, perfiles, grupos, activos, horarios, criticidad, aprobaciones u otros criterios equivalentes definidos por la ENTIDAD.

S20.5. Requisitos técnicos y de integración

S20.5.1. Soporte multiplataforma: EL PROVEEDOR debe soportar, como mínimo, Windows (AD), Linux, bases de datos, dispositivos de red y nube pública (Oracle, Azure, GCP) o equivalentes presentes en la ENTIDAD.

S20.5.2. API-First: EL PROVEEDOR debe proveer capacidades API-First para automatización (aprovisionamiento, flujos de aprobación, onboarding/offboarding y/o integración con ITSM institucional).

S20.5.3. Alta disponibilidad (HA) y break-glass: EL PROVEEDOR debe asegurar mecanismos de redundancia y contingencia. En caso de falla total del PAM, debe existir un protocolo físico o lógico seguro de acceso a sistemas críticos sin pasar por la herramienta, que deje rastro y sea gobernado por la ENTIDAD (break-glass), conforme a procedimiento aprobado.

S20.5.4. Escalabilidad: EL PROVEEDOR debe garantizar capacidad de operación y escalabilidad acorde al número de cuentas, sesiones, usuarios privilegiados, activos críticos y casos de uso definidos por la ENTIDAD.

S20.5.5. Integración con plataformas: EL PROVEEDOR debe integrar o interoperar con plataformas de monitoreo, automatización, respuesta o gestión, tales como SIEM, SOAR, ITSM, IAM, MFA, SSO, ZTNA u otras equivalentes integradas y las propias de la ENTIDAD.

S20.6. Integración con SOC como servicio (SIEM/SOAR)

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S20.6.1. (SIEM) EL PROVEEDOR debe enviar al SIEM del SOC como servicio los eventos, veredictos (cuando aplique), IoCs y evidencias del PAM por mecanismos soportados (API/syslog/webhook o conectores estándar), permitiendo correlación multi-fuente y trazabilidad end-to-end.

S20.6.2. Los eventos enviados al SIEM deben ser explicables y trazables (incluyendo, cuando aplique, artefacto/fuente/técnica ATT&CK/score/evidencia), conforme a los lineamientos del SOC.

S20.6.3. (SOAR) EL PROVEEDOR debe habilitar disparadores para playbooks SOAR relacionados con PAM, como bloqueo o terminación de sesión, revocación de credenciales, rotación forzada, deshabilitación temporal de cuenta privilegiada u otras acciones definidas por la ENTIDAD, bajo gobernanza (automático preaprobado o con aprobación).

S20.7. ITSM institucional (system of record, tickets automáticos y CMDB)

S20.7.1. El PROVEEDOR debe suministrar e implementar el mecanismo técnico de integración entre el PAM y la herramienta ITSM institucional, de modo que los incidentes/casos definidos por la ENTIDAD generen automáticamente ticket/caso en ITSM con severidad/prioridad, evidencias, IoCs y acciones. La gestión, configuración y administración de la herramienta ITSM es responsabilidad exclusiva de la ENTIDAD; el PROVEEDOR garantiza únicamente la integración técnica y su correcto funcionamiento.

S20.7.2. La integración debe soportar, como mínimo: creación automática de tickets, actualización automática con estados/evidencias, sincronización de estados (bidireccional cuando el ITSM lo permita), trazabilidad de transacciones e idempotencia (no duplicación), con colas/reintentos y alertas por fallas de integración.

S20.7.3. La integración debe realizarse mediante mecanismos estándar soportados por el ITSM (APIs/servicios/webhooks o equivalentes), evitando requisitos direccionadores por marca.

S20.7.4. EL PROVEEDOR debe consumir la CMDB de la ENTIDAD para enriquecer eventos/alertas y tickets con criticidad, propietario, servicio relacionado, ambiente y metadatos del CI; y vincular cada ticket al CI correspondiente en CMDB para priorización automática y reportes.

S20.7.5. EL PROVEEDOR debe reportar inconsistencias CMDB como tickets de mejora/problema según el modelo ITSM de la ENTIDAD.

S20.7.6. Si la ENTIDAD migra de ITSM durante la ejecución, EL PROVEEDOR debe adaptar la integración al nuevo ITSM en el plazo definido contractualmente, sin afectar la operación 24x7 y soportando operación paralela si la ENTIDAD lo exige.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S20.8. Integración con herramienta de Observabilidad de la ENTIDAD

S20.8.1. EL PROVEEDOR debe integrar el servicio PAM con la herramienta de Observabilidad de la ENTIDAD para visibilidad operacional, incluyendo como mínimo: salud y disponibilidad del servicio, estado de conectores/integraciones (SIEM/SOAR/ITSM/IAM cuando aplique), colas/reintentos y métricas agregadas (número de sesiones privilegiadas, sesiones grabadas, sesiones terminadas por supervisión, rotaciones ejecutadas, fallas de rotación, uso de break-glass), conforme defina la ENTIDAD.

S20.9. Reportes y cumplimiento

S20.9.1. Tableros de cumplimiento: EL PROVEEDOR debe proveer tableros/reportes operativos, de cumplimiento, auditoría o investigación en formatos utilizables por la ENTIDAD.

S20.9.2. Alertas de anomalías: EL PROVEEDOR debe generar alertas ante actividades no autorizadas, anómalas, fuera de política o sospechosas relacionadas con accesos privilegiados y ponerlas a disposición del SOC (SIEM/SOAR) según el modelo de integración.

S20.10. Pruebas de aceptación (PAM + SOC/ITSM/Observabilidad)

S20.10.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencien como mínimo:

a) Bóveda, préstamo controlado (check-in/check-out) y rotación automática de credenciales.
b) Aislamiento de sesión vía proxy/jump y grabación de sesiones RDP/SSH/web (video + comandos).
c) Monitoreo en vivo y finalización de sesión por supervisión; y búsqueda por comandos en grabaciones.
d) ZSP y JIT con flujos de aprobación y MFA para portal PAM, conforme a políticas.
e) Integración SIEM y trazabilidad SIEM ↔ ITSM (validación de campos mínimos): EL PROVEEDOR debe evidenciar en el SIEM del SOC como servicio la recepción de eventos PAM representativos (checkout/check-in de credencial, rotación automática, inicio/fin de sesión privilegiada por proxy/jump, grabación de sesión, aprobación/denegación, terminación de sesión por supervisión y/o uso de break-glass cuando aplique), verificando que cada evento contiene los campos mínimos definidos en S20.11.2 (o su equivalente funcional en el conector) y que los eventos son explicables y trazables (incluyendo, cuando aplique, artefacto/fuente/técnica ATT&CK/score/evidencia).
Adicionalmente, EL PROVEEDOR debe validar la trazabilidad end-to-end SIEM ↔ ITSM para los casos definidos por la ENTIDAD, evidenciando que el evento/caso en SIEM referencia el TicketId (y/o CorrelationId/CaseId) del ITSM, y que el ticket en ITSM referencia de

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

forma cruzada el CaseId/CorrelationId del SIEM/SOAR cuando aplique, conforme al esquema institucional de integración y trazabilidad (incluida idempotencia/no duplicación y trazabilidad de transacciones).
La evidencia debe presentarse mediante capturas y/o exportaciones del SIEM y del ITSM, y/o evidencia documental del conector, conforme al procedimiento de aceptación de la ENTIDAD.
e.1) IoCs (cuando aplique): EL PROVEEDOR debe evidenciar que los IoCs asociados a eventos PAM (cuando existan) pueden ser extraídos, normalizados y exportados en formatos estándar (STIX/TAXII o equivalente) para consumo por SIEM/SOAR/TIP cuando aplique, conforme a S20.11.3.

f) Integración SOAR (validación funcional + gobernanza + trazabilidad): EL PROVEEDOR debe evidenciar que el SOAR del SOC como servicio recibe las alertas del SIEM y otras fuentes definidas (cuando aplique) por mecanismos soportados (API/syslog/webhook o conectores), y que realiza ingesta y normalización, deduplicación y correlación para su gestión.
Adicionalmente, EL PROVEEDOR debe evidenciar que el SOAR ejecuta al menos un (1) playbook asociado a PAM, bajo el modelo de gobernanza definido por la ENTIDAD (automático preaprobado o con aprobación), incluyendo como mínimo un caso controlado de: (i) terminación de sesión privilegiada o bloqueo/contención y/o (ii) rotación forzada/revocación de credenciales; con registro de la ejecución (pasos, tiempos, resultado) y evidencias asociadas.
f.1) Trazabilidad SOAR ↔ ITSM: EL PROVEEDOR debe evidenciar que el SOAR se integra con el ITSM institucional para crear automáticamente tickets de Incidente y tareas asociadas, y cuando aplique, tickets de Cambio (incluido cambio de emergencia) y Problema; y que sincroniza bidireccionalmente (ID cruzado SOAR/SIEM ↔ ITSM, estados, severidad/prioridad, bitácora y evidencias). La evidencia debe demostrar idempotencia (no duplicación), colas/reintentos y alertas por fallas de integración.

g) Integración Observabilidad: visualización en Observabilidad del estado del servicio e integraciones y métricas operacionales definidas.

S20.10.2. EL PROVEEDOR debe consolidar resultados en acta y dossier de evidencias conforme al procedimiento de aceptación definido por la ENTIDAD.

S20.11. Campos mínimos de eventos PAM para SIEM (SOC como servicio)

S20.11.1. EL PROVEEDOR debe garantizar que los logs, eventos y alertas generados por el servicio PAM y enviados al SIEM del SOC como servicio sean explicables y trazables, permitiendo correlación multifuente. En particular, los eventos deben incluir, cuando aplique, artefacto, fuente, técnica ATT&CK, score/confianza y evidencia (o referencias seguras a evidencias).-

S20.11.2. Los eventos/alertas enviados al SIEM deben incluir, como mínimo, los siguientes campos (o su equivalente funcional en el formato del conector), sin perjuicio de campos adicionales

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		del fabricante y preservando la confidencialidad según políticas de la ENTIDAD: a) EventId y tipo de registro (evento/alerta/veredicto). b) timestamp (fecha/hora con zona horaria). c) Source y componente PAM que originó el evento (como bóveda/vault, rotación, descubrimiento, checkout/check-in, proxy/jump, grabación, aprobación, break-glass, etc.). d) ActivityType y Action (como creación/actualización, rotación, préstamo, inicio/fin de sesión, terminación por supervisión, aprobación/denegación, uso de break-glass), cuando aplique. e) Actor: usuario solicitante/ejecutor (y grupo/rol cuando aplique) y método de autenticación (como MFA/SSO cuando aplique). f) PrivAccountId: identificador de la cuenta/credencial afectada (sin exponer secretos) y estado (rotada, revocada, expirada, prestada), cuando aplique. g) TargetAsset/CI: activo objetivo (hostname/IP/FQDN) y, cuando aplique, CIId o referencia a CMDB (criticidad/servicio/ambiente) según defina la ENTIDAD. h) SessionId y contexto de sesión: protocolo (RDP/SSH/WEB u otro), origen de conexión y estado de sesión, cuando aplique. i) Evidence: referencia segura a grabación de sesión (video) y logs de comandos (texto) cuando aplique, sin exponer contenido sensible en claro. j) CommandIndicator: marcador/atributo buscable asociado a comandos/acciones relevantes (cuando aplique), sin exponer información sensible en claro. k) PolicyId/RuleId y condición de control (horario, rol, aprobación, JIT/ZSP cuando aplique) u otros criterios definidos por la ENTIDAD. l) Approval: identificador de solicitud, aprobador, resultado (aprobado/denegado) y justificación (cuando aplique). m) Severity/Criticality y racional, conforme al modelo definido por la ENTIDAD. n) ConfidenceScore cuando el fabricante/servicio lo soporte y su justificación. o) IoCs asociados cuando existan (IPs, dominios, URLs, hashes/artefactos relacionados), con tipo y valor. p) Correlación inter-herramienta (CorrelationId/CaseId) y, cuando aplique, referencia cruzada a SOAR e ITSM (TicketId) para trazabilidad end-to-end (SIEM ↔ SOAR ↔ ITSM), incluyendo identificador del playbook/automatización ejecutada en SOAR (SOARPlaybookId/AutomationId o equivalente) y su versión, para auditoría y bitácora de acciones. S20.11.3. EL PROVEEDOR debe soportar la extracción, normalización y gestión de IoCs (hashes, dominios, IPs, URLs) y permitir su exportación en formatos estándar (STIX/TAXII o equivalente) para consumo por SIEM/SOAR/TIP cuando aplique.
S21.	Servicio de Seguridad en IPV6 S21.1. Objeto y alcance S21.1.1. EL PROVEEDOR debe prestar un servicio especializado de seguridad aplicable al protocolo IPv6 para soportar la implementación y operación segura de IPv6 en la ENTIDAD, incluyendo diagnóstico, endurecimiento, configuración	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

de controles, monitorización, transferencia de conocimiento, soporte y seguimiento durante el plazo de ejecución contractual.

S21.1.2. EL PROVEEDOR debe disponer de un especialista en seguridad aplicable a IPv6, quien trabaja coordinadamente con el equipo de implementación y con los responsables de seguridad de la ENTIDAD para definir, ejecutar y mantener los mecanismos de seguridad aplicables.

S21.2. Fase de diagnóstico y endurecimiento (hardening)

S21.2.1. Auditoría de superficie de exposición: EL PROVEEDOR debe identificar todos los dispositivos, servicios y segmentos con IPv6 habilitado, inventariar su rol y validar configuraciones necesarias y no necesarias que incrementen la exposición o impliquen vulnerabilidades.

S21.2.2. Revisión de configuración IPv6: EL PROVEEDOR debe revisar y documentar, como mínimo, el estado de direccionamiento, anuncios, autoconfiguración, rutas, servicios de transición y parámetros de seguridad por interfaz y por segmento, definiendo un plan de remediación priorizado.

S21.2.3. RA Guard (Router Advertisement Guard): EL PROVEEDOR debe implementar mecanismos para evitar anuncios de router no autorizados y ataques de suplantación del router, mediante RA Guard o controles equivalentes en la infraestructura correspondiente, conforme al diseño de red de la ENTIDAD.

S21.2.4. Control de direccionamiento: EL PROVEEDOR debe establecer y documentar políticas de asignación de direcciones (DHCPv6 frente a SLAAC, o combinación controlada), y asegurar que las direcciones de servidores críticos se gestionan conforme a una política aprobada por la ENTIDAD, evitando asignaciones no controladas y reduciendo la predictibilidad cuando aplique.

S21.2.5. Gestión de servicios no requeridos: EL PROVEEDOR debe deshabilitar o restringir funcionalidades IPv6 no requeridas en equipos, sistemas operativos y dispositivos de red, cuando dichas funcionalidades incrementen la superficie de exposición y exista aprobación del equipo técnico responsable de la ENTIDAD.

S21.2.6. Entregables de diagnóstico: EL PROVEEDOR debe entregar un informe de diagnóstico que incluya inventario de exposición, hallazgos, riesgos, recomendaciones, plan de remediación y evidencias mínimas de verificación.

S21.3. Gestión de seguridad perimetral y filtrado

S21.3.1. Coordinación con seguridad perimetral: EL PROVEEDOR debe ejecutar estas actividades en conjunto con el equipo responsable de seguridad perimetral de la ENTIDAD, asegurando consistencia de políticas entre IPv4 e IPv6, sin afectar la continuidad operativa.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S21.3.2. Políticas de firewall “default deny”: EL PROVEEDOR debe definir y configurar reglas estrictas de entrada y salida para IPv6 bajo el principio de denegación por defecto, evitando supuestos de seguridad derivados de NAT en IPv4.

S21.3.3. Gestión crítica de ICMPv6: EL PROVEEDOR debe implementar reglas de control de ICMPv6 basadas en buenas prácticas, filtrando únicamente lo riesgoso sin romper la conectividad, garantizando el funcionamiento de mensajes necesarios para la operación del protocolo, incluido el soporte de MTU cuando aplique.

S21.3.4. Filtrado de cabeceras de extensión: EL PROVEEDOR debe configurar los equipos de seguridad para inspeccionar, restringir o descartar paquetes con cabeceras de extensión maliciosas o anómalas que intenten evadir controles, conforme a capacidades del fabricante y al análisis de riesgo aprobado por la ENTIDAD.

S21.3.5. Endurecimiento de dispositivos perimetrales: EL PROVEEDOR debe validar que los dispositivos perimetrales y de borde aplican controles equivalentes para IPv6 a los existentes para IPv4, incluyendo control por zonas, segmentación y aplicación de políticas por servicio.

S21.4. Monitorización y visibilidad

S21.4.1. Monitorización dual-stack: EL PROVEEDOR debe asegurar que los sistemas de detección y prevención de intrusos (IDS/IPS) y el SIEM procesan logs y eventos de IPv6 con prioridad y cobertura equivalente a IPv4, habilitando correlación y visibilidad unificada.

S21.4.2. Detección de túneles no autorizados: EL PROVEEDOR debe monitorizar y bloquear mecanismos de transición automáticos o no autorizados que permitan eludir controles corporativos, incluyendo túneles de IPv6 sobre IPv4 cuando aplique, conforme a las políticas definidas por la ENTIDAD.

S21.4.3. Gestión de privacidad (privacy extensions): EL PROVEEDOR debe configurar y supervisar el uso de direcciones temporales en equipos finales cuando aplique, garantizando un equilibrio entre privacidad y trazabilidad, de acuerdo con los requerimientos de auditoría e investigación definidos por la ENTIDAD.

S21.4.4. Telemetría y trazabilidad: EL PROVEEDOR debe garantizar que las fuentes de logs incluyen los campos necesarios para trazabilidad (origen/destino IPv6, usuario cuando aplique, activo, política aplicada, acción del control y sello de tiempo), conforme al estándar de correlación del SOC.

S21.5. Labores operativas y de cumplimiento

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		S21.5.1. Plan de direccionamiento seguro: EL PROVEEDOR debe diseñar y documentar un plan de direccionamiento y subneteo IPv6 que dificulte el escaneo de red y que esté alineado con la arquitectura y operación de la ENTIDAD, incluyendo criterios de asignación y segmentación. S21.5.2. Capacitación y transferencia de conocimiento: EL PROVEEDOR debe capacitar al equipo de soporte técnico de la ENTIDAD en resolución de problemas específicos de IPv6, incluyendo verificación de conectividad, diagnóstico de anuncios, rutas, MTU y fallos típicos en operación dual-stack. S21.5.3. Actualización de planes de continuidad y respuesta: EL PROVEEDOR debe asegurar que, ante un incidente o fallo de seguridad, los protocolos y procedimientos de respuesta cubren explícitamente tráfico IPv6, incluyendo contención, bloqueo, preservación de evidencias y restauración del servicio, conforme al modelo de operación definido por la ENTIDAD. S21.5.4. Seguimiento y mejora continua: EL PROVEEDOR debe realizar seguimiento periódico de la postura de seguridad IPv6, registrar hallazgos y planes de acción, y ejecutar ajustes (tuning) controlados y auditables durante la vigencia del contrato. S21.6. Integración con operación de seguridad, ITSM y observabilidad S21.6.1. Integración con SOC: EL PROVEEDOR debe alinear la operación del servicio IPv6 con el SOC como servicio, garantizando que los eventos relevantes de IPv6 se gestionan conforme a la operación de monitorización, triaje, investigación y respuesta de la ENTIDAD. S21.6.2. ITSM institucional: EL PROVEEDOR debe gestionar hallazgos, cambios y actividades del servicio IPv6 mediante la herramienta ITSM institucional como repositorio oficial de tickets, asegurando trazabilidad de solicitudes, aprobaciones, evidencias, cambios y cierres, conforme al procedimiento definido por la ENTIDAD. S21.6.3. Observabilidad: EL PROVEEDOR debe integrar métricas y estado operativo asociados a controles y servicios IPv6 en la herramienta de observabilidad de la ENTIDAD, incluyendo salud de integraciones, disponibilidad de fuentes de logs y estado de controles críticos implementados, conforme a los casos de uso definidos por la ENTIDAD. S21.7. Pruebas de aceptación S21.7.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencian, como mínimo: a) Inventario validado de superficie de exposición IPv6, con hallazgos y plan de remediación. b) Implementación efectiva de RA Guard o control equivalente y verificación mediante casos controlados.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		c) Aplicación de políticas de firewall con denegación por defecto en IPv6, con evidencia de reglas y validación de tráfico permitido/bloqueado. d) Configuración de reglas de ICMPv6 que mantienen conectividad y controlan lo riesgoso, con evidencia de pruebas de conectividad. e) Controles frente a cabeceras de extensión, con evidencia de configuración y validación de comportamiento. f) Evidencia de monitorización dual-stack: confirmación de recepción y consulta de eventos/logs IPv6 en IDS/IPS y SIEM, con ejemplos de eventos. g) Evidencia de detección y bloqueo de mecanismos de transición no autorizados cuando aplique. h) Evidencia de parametrización y supervisión de privacy extensions cuando aplique, manteniendo trazabilidad para auditoría. i) Evidencia de capacitación impartida y material entregado al equipo de soporte. j) Evidencia de actualización de procedimientos de respuesta y continuidad que incluyen IPv6. S21.7.2. EL PROVEEDOR debe consolidar resultados en un acta y un dossier de evidencias conforme al procedimiento de aceptación definido por la ENTIDAD. S21.8. Criterios de aceptación S21.8.1. El servicio de seguridad en IPv6 se acepta contra evidencias mínimas verificables, consolidadas en un acta de aceptación y un dossier de evidencias, conforme al procedimiento de aceptación definido por la ENTIDAD. S21.8.2. Para la aceptación, EL PROVEEDOR debe entregar y dejar disponibles las siguientes evidencias mínimas: a) Informe de diagnóstico y endurecimiento aprobado por la ENTIDAD, que incluye inventario de superficie de exposición IPv6, hallazgos, riesgos, recomendaciones y plan de remediación priorizado, con evidencias de verificación. b) Evidencia de implementación y operación de RA Guard o control equivalente, con casos controlados documentados y resultados, incluyendo validación de mitigación de anuncios de router no autorizados. c) Evidencia de políticas de firewall para IPv6 bajo denegación por defecto, incluyendo reglas vigentes, pruebas de tráfico permitido y bloqueado y evidencias de control perimetral, sin afectar la continuidad operativa. d) Evidencia de gestión de ICMPv6 basada en buenas prácticas, incluyendo reglas vigentes y pruebas de conectividad que demuestran operación correcta del protocolo y control de mensajes riesgosos. e) Evidencia de inspección, restricción o descarte de cabeceras de extensión cuando aplique, con configuración vigente y validación de comportamiento. f) Evidencia de monitorización dual-stack que demuestra recepción y consulta de logs/eventos IPv6 en IDS/IPS y SIEM con prioridad equivalente a IPv4, incluyendo ejemplos de eventos y trazabilidad mínima.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		g) Evidencia de detección y bloqueo de mecanismos de transición no autorizados cuando aplique, con registros de control y resultados de verificación. h) Evidencia de parametrización y supervisión de direcciones temporales (privacy extensions) cuando aplique, garantizando trazabilidad suficiente para auditoría e investigación conforme a lo definido por la ENTIDAD. i) Plan de direccionamiento seguro aprobado por la ENTIDAD, incluyendo criterios de subneteo/segmentación y lineamientos de asignación. j) Evidencia de capacitación impartida y transferencia de conocimiento al equipo de soporte, incluyendo material entregado y registro de asistencia. k) Evidencia de actualización de procedimientos de continuidad y respuesta a incidentes que incluyen explícitamente tráfico IPv6, con control de cambios y responsables. l) Evidencia de trazabilidad operativa en ITSM para hallazgos, cambios y actividades del servicio IPv6, incluyendo tickets, aprobaciones, evidencias y cierres, conforme a la herramienta ITSM institucional. m) Evidencia de integración en la herramienta de observabilidad de la ENTIDAD, incluyendo estado de controles críticos implementados, disponibilidad de fuentes de logs y salud de integraciones, conforme a los casos de uso definidos por la ENTIDAD. S21.8.3. EL PROVEEDOR debe consolidar las evidencias anteriores en un dossier estructurado y referenciado al acta de aceptación, de modo que la ENTIDAD puede auditar el cumplimiento, replicar las verificaciones y mantener trazabilidad durante la operación.
	S22.	Servicio de Seguridad para SD-WAN Integrado con SOC, ITSM y Observabilidad S22.1. Objeto y alcance S22.1.1. EL PROVEEDOR debe implementar y operar controles de seguridad para la SD-WAN de la ENTIDAD, garantizando visibilidad, segmentación, aplicación de políticas por identidad, auditoría, y respuesta ante degradación y eventos de seguridad, conforme al modelo de operación definido por la ENTIDAD. S22.1.2. EL PROVEEDOR debe alinear la operación de seguridad SD-WAN con el SOC como servicio, gestionar los casos mediante la herramienta ITSM institucional y publicar telemetría y estado en la herramienta de observabilidad de la ENTIDAD, según los mecanismos y lineamientos definidos. S22.2. Ingeniería de tráfico basada en analítica SD-WAN S22.2.1. EL PROVEEDOR debe disponer de analítica SD-WAN que permita evaluar desempeño por aplicación, enlace y categoría de sede, y debe generar reportes operativos y ejecutivos que soporten la gestión de niveles de servicio.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S22.2.2. EL PROVEEDOR debe garantizar la disponibilidad de tableros y métricas que permitan, como mínimo: latencia, pérdida, jitter, throughput, disponibilidad por enlace, desempeño por aplicación, eventos de conmutación, degradación y cumplimiento de políticas por categoría.

S22.2.3. EL PROVEEDOR debe mantener históricos de las métricas y eventos definidos por la ENTIDAD, asegurando que puedan ser consultados para auditorías, análisis de tendencia y aplicación de acciones correctivas.

S22.3. Inspección profunda de tráfico e identificación de aplicaciones (DPI) y conmutación por degradación

S22.3.1. EL PROVEEDOR debe garantizar capacidades locales en cada sede para inspección profunda de tráfico e identificación y clasificación de aplicaciones mediante inspección profunda de tráfico, DPI o mecanismo funcionalmente equivalente, de forma que la política se aplique en el punto de acceso SD-WAN.

S22.3.2. EL PROVEEDOR debe implementar priorización por aplicación y políticas de conmutación automática ante degradación del enlace, con definición de umbrales por la ENTIDAD y trazabilidad de los eventos de degradación y de los cambios de ruta.

S22.3.3. EL PROVEEDOR debe asegurar que la conmutación y priorización no degradan la disponibilidad de aplicaciones críticas y que la política se aplica consistentemente en todas las sedes incluidas en el alcance.

S22.4. Seguridad continua en puntos de acceso WAN (SD-WAN)

S22.4.1. EL PROVEEDOR debe disponer de capacidades para análisis de vulnerabilidades, evaluación de configuración segura y monitoreo continuo de seguridad en los puntos de acceso WAN/SD-WAN (CPE/edge), incluyendo detección de configuraciones débiles, exposición de servicios y desviaciones de la línea base.

S22.4.2. EL PROVEEDOR debe generar hallazgos priorizados con plan de acción y debe registrarlos como casos en ITSM cuando la ENTIDAD lo determine.

S22.4.3. EL PROVEEDOR debe implementar controles para gestión de superficie de exposición en el borde SD-WAN, incluyendo deshabilitación o restricción de servicios no utilizados y endurecimiento de administración.

S22.5. Aplicación automática de perfiles de navegación por usuario

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S22.5.1. EL PROVEEDOR debe garantizar que los perfiles de navegación de los funcionarios se apliquen automáticamente en la red de cada sede, preferiblemente sin instalar software adicional en los computadores, utilizando capacidades de SD-WAN y controles locales de seguridad (firewalls, filtros locales o equivalentes) y el modelo de identidad institucional. Se admiten igualmente los mecanismos previstos en el numeral S22.5.4.

S22.5.2. EL PROVEEDOR debe integrar la solución con el directorio institucional para soportar políticas basadas en identidad (usuario o grupo) aplicables al control de navegación, evitando requerir credenciales adicionales para identificar el flujo cuando aplique. La identificación de usuario o grupo no constituye un requisito obligatorio para las funciones de enrutamiento o calidad de servicio del SD-WAN, las cuales podrán definirse por criterios técnicos tales como aplicación (DPI/L7), clase de servicio, segmento, origen/destino, desempeño de enlaces y cumplimiento de SLA; su uso para estos fines podrá ofrecerse como capacidad adicional de la solución.

S22.5.3. EL PROVEEDOR debe asegurar que la aplicación de perfiles de navegación se alinea con las normas y políticas de seguridad definidas por la ENTIDAD en el anexo de seguridad vigente.

S22.5.4. Para las capacidades de aplicación de perfiles de navegación e identidad de usuario descritas en los numerales S22.5.1 a S22.5.3, se aceptarán arquitecturas que las implementen mediante agentes, túneles, navegador seguro u otros mecanismos funcionalmente equivalentes, siempre que garanticen trazabilidad, aplicación de políticas e integración con los servicios institucionales definidos. Estos mecanismos complementan y no sustituyen la arquitectura SD-WAN ni sus funciones de transporte, enrutamiento, calidad de servicio, segmentación e inspección de tráfico definidas en el Anexo Técnico 1 — Conectividad y en el presente anexo; su adopción no exime al PROVEEDOR de mantener el overlay SD-WAN y los controles de seguridad de red por sede, ni de garantizar la cobertura de los dispositivos que no admiten agente (impresoras, cámaras, IoT, equipos no gestionados e invitados) mediante los controles de red correspondientes. Los mecanismos adoptados deberán gestionarse de forma centralizada, no podrán ser deshabilitados por el usuario final y deberán reportar sus eventos al SOC (SIEM) y a la herramienta de observabilidad institucional.

S22.6. Segmentación de acceso por origen y gestión de servicios no utilizados

S22.6.1. EL PROVEEDOR debe implementar segmentación de acceso por origen, zona, VLAN u otro mecanismo equivalente, y debe aplicar políticas que restrinjan servicios no utilizados, reduzcan exposición y eviten movimientos laterales no autorizados.

S22.6.2. EL PROVEEDOR debe mantener un inventario de servicios habilitados en el borde SD-WAN y debe gestionar

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

cambios mediante control de cambios y evidencias, conforme a ITSM.

S22.7. Identidad, acceso y privilegios (MFA y control de roles)

S22.7.1. EL PROVEEDOR debe implementar mecanismos de autenticación estrictos y MFA para el acceso a la plataforma de administración SD-WAN.

S22.7.2. EL PROVEEDOR debe aplicar control de privilegios y roles para administración SD-WAN, bajo el principio de mínimo privilegio, y debe registrar auditoría completa de accesos y cambios.

S22.7.3. EL PROVEEDOR debe soportar que la gestión de privilegios se ejecute de forma local o a través del servicio PAM cuando la ENTIDAD lo disponga, garantizando trazabilidad de las acciones administrativas.

S22.8. Integración con SOC como servicio (SIEM/SOAR)

S22.8.1. EL PROVEEDOR debe permitir el envío de logs y eventos relevantes de SD-WAN a la herramienta SIEM del SOC, de modo que se habilite correlación e investigación.

S22.8.2. EL PROVEEDOR debe asegurar que los logs/eventos de SD-WAN incluyen campos mínimos de trazabilidad definidos por la ENTIDAD, incluyendo origen/destino, identidad cuando aplique, aplicación identificada, política aplicada, acción, sello de tiempo, enlace utilizado y resultado (permitido/bloqueado/conmutado).

S22.8.3. EL PROVEEDOR debe permitir la ejecución de tareas automatizadas enviadas por la herramienta SOAR cuando aplique, conforme a la gobernanza definida por la ENTIDAD, incluyendo registro de la acción, resultado y evidencias.

S22.9. ITSM institucional

S22.9.1. EL PROVEEDOR debe gestionar alertas relevantes, incidentes, requerimientos y solicitudes de cambio asociadas a SD-WAN mediante la herramienta ITSM de la ENTIDAD.

S22.9.2. EL PROVEEDOR debe crear, actualizar y cerrar tickets en ITSM mediante integración soportada, garantizando trazabilidad completa, evidencias, bitácora y auditoría de acciones.

S22.9.3. EL PROVEEDOR debe asegurar que los tickets incluyen, como mínimo: clasificación, severidad/prioridad, activo o sede afectada, enlace, aplicación afectada, evidencia técnica, acciones ejecutadas, responsables y cierre.

S22.10. Integración con la herramienta de observabilidad de la ENTIDAD

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S22.10.1. EL PROVEEDOR debe integrar métricas, logs y estado operativo de SD-WAN en la herramienta de observabilidad de la ENTIDAD, incluyendo disponibilidad por sede/enlace, degradación de enlaces, conmutación, desempeño por aplicación, salud de integraciones y estado de políticas.

S22.10.2. EL PROVEEDOR debe asegurar que la observabilidad permite evidenciar cumplimiento de niveles de servicio y periodos de degradación, soportando la aplicación de penalizaciones cuando corresponda.

S22.11. Pruebas de aceptación

S22.11.1. EL PROVEEDOR debe ejecutar y documentar pruebas de aceptación acordadas con la ENTIDAD que evidencian, como mínimo:

a) Analítica SD-WAN por aplicación/enlace/categoría: disponibilidad de tableros, consulta de métricas y exportación de reporte operativo.
b) Identificación y clasificación local de aplicaciones mediante DPI o mecanismo funcionalmente equivalente: evidencia de identificación de aplicaciones y aplicación de política por aplicación.
c) Priorización por aplicación: evidencia de clasificación y priorización aplicada, con medición comparativa antes/después para una aplicación definida por la ENTIDAD.
d) Conmutación automática ante degradación: evidencia del evento de degradación, el cambio de ruta y la estabilización de la métrica afectada, con registro del enlace anterior y el enlace posterior.
e) Seguridad continua en borde SD-WAN: evidencia de evaluación de configuración segura y/o hallazgos de vulnerabilidades del edge, con plan de acción.
f) Aplicación automática de perfiles de navegación por identidad: evidencia de aplicación por usuario o grupo mediante el mecanismo propio de la arquitectura ofertada (desde la red, agentes, túneles, navegador seguro o mecanismos funcionalmente equivalentes, conforme al numeral S22.5.4), con registros de política aplicada.
g) Segmentación por origen: evidencia de segmentación implementada y validación de restricción de acceso entre segmentos según política.
h) Integración SIEM: evidencia de recepción y consulta de logs/eventos SD-WAN en el SIEM del SOC, con trazabilidad mínima (aplicación, enlace, sede, acción).
i) Integración SOAR cuando aplique: evidencia de ejecución de al menos una automatización asociada a SD-WAN o seguridad perimetral local, con resultado y registro.
j) Integración ITSM: evidencia de tickets creados/actualizados para incidentes, requerimientos y cambios SD-WAN, con evidencias técnicas adjuntas y trazabilidad de cierre.
k) Integración observabilidad: evidencia de visualización en observabilidad de métricas SD-WAN, eventos de degradación y conmutación, y estado de salud del servicio.

S22.11.2. EL PROVEEDOR debe consolidar resultados en un acta y un dossier de evidencias conforme al procedimiento de aceptación definido por la ENTIDAD.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

S22.12. Criterios de aceptación

S22.12.1. El servicio se acepta contra evidencias mínimas verificables, consolidadas en un acta de aceptación y un dossier de evidencias, conforme al procedimiento definido por la ENTIDAD.

S22.12.2. Para que el servicio sea aceptado, EL PROVEEDOR debe cumplir simultáneamente los siguientes criterios:

A. Criterios de aceptación funcional (operación y seguridad)
A.1 Analítica SD-WAN: Se acepta si la ENTIDAD puede consultar métricas por aplicación, enlace y categoría, y si el PROVEEDOR entrega un reporte consolidado que incluya, como mínimo, indicadores de desempeño y eventos de conmutación y degradación del periodo evaluado.
A.2 Identificación y clasificación local de aplicaciones: Se acepta si se evidencia identificación de aplicaciones en al menos una sede de prueba y si las políticas por aplicación se aplican con resultado verificable (permitir/bloquear/priorizar).
A.3 Conmutación por degradación: Se acepta si se evidencia un caso controlado de degradación en enlace y la conmutación automática según umbral definido, con registro de evento, cambio de ruta y resultado sobre la métrica.
A.4 Perfiles de navegación por identidad: se acepta si las políticas se aplican automáticamente por usuario o grupo mediante el mecanismo propio de la arquitectura ofertada, incluido control desde red, agente, túnel, navegador seguro o mecanismo funcionalmente equivalente, garantizando trazabilidad y administración centralizada.

A.5 Segmentación por origen: Se acepta si existe segmentación implementada y se comprueba restricción efectiva de accesos no autorizados entre segmentos, con reglas vigentes y evidencia de prueba.
A.6 Gestión de servicios no utilizados: Se acepta si el inventario de servicios del borde SD-WAN está documentado, si los servicios no requeridos se restringen o deshabilitan conforme a aprobación, y si el cambio queda trazado.

B. Criterios de aceptación de integración (SOC, ITSM y observabilidad)
B.1 SIEM: Se acepta si el SIEM recibe eventos/logs SD-WAN con trazabilidad mínima exigida por la ENTIDAD y si se demuestra consulta y correlación básica durante la prueba.
B.2 SOAR cuando aplique: Se acepta si se demuestra ejecución de una automatización definida por la ENTIDAD, con evidencia de entrada (alerta/evento), acción ejecutada y resultado, y registro de auditoría.
B.3 ITSM: Se acepta si se evidencia creación y actualización de tickets para casos definidos por la ENTIDAD, incluyendo evidencias adjuntas, bitácora y cierre; y si se evidencia gestión de cambios cuando aplique.
B.4 Observabilidad: Se acepta si se visualizan métricas SD-WAN y estado de salud del servicio y sus integraciones, y si se pueden identificar periodos de degradación y eventos de conmutación en línea de tiempo.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

C. Criterios de aceptación de evidencias
C.1 Acta de aceptación: Se acepta si el acta está suscrita por las partes según el procedimiento de la ENTIDAD y contiene el alcance probado, resultados y desviaciones.
C.2 Dossier de evidencias: Se acepta si el dossier incluye capturas/exportaciones de tableros de analítica, registros de eventos de conmutación/degradación, evidencias de políticas por identidad y por aplicación, evidencias de segmentación, evidencias SIEM/SOAR cuando aplique, evidencias ITSM y evidencias de observabilidad.
C.3 Control de cambios: Se acepta si las modificaciones realizadas sobre políticas y configuraciones durante las pruebas quedan registradas y trazadas conforme al procedimiento definido por la ENTIDAD.

S22.12.3. Si alguno de los criterios anteriores no se cumple, EL PROVEEDOR debe registrar el hallazgo en ITSM, presentar plan de remediación con fechas y evidencias, y repetir las pruebas afectadas hasta lograr aceptación conforme al procedimiento de la ENTIDAD.

S23. Servicio de administración de las herramientas de seguridad de Microsoft 365 integrado al SOC como servicio, Observabilidad e ITSM

S23.1. Objeto y alcance

El PROVEEDOR debe prestar el servicio de administración, operación, optimización y mejora continua de las herramientas de seguridad de Microsoft de la ENTIDAD, incluyendo como mínimo Microsoft Entra ID, Microsoft Purview, Microsoft Sentinel, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, Microsoft Defender for Cloud, las capacidades premium de Microsoft Intune que se encuentren habilitadas/licenciadas/activas, y las capacidades de identidad, gobierno, acceso y verificación de la familia Microsoft Entra que se encuentren habilitadas/licenciadas/activas durante la ejecución del contrato; así como los componentes on-premises o híbridos requeridos para su operación, integración o sensorización, incluyendo Directorio Activo (Active Directory), sensores, conectores, agentes y dependencias asociadas cuando aplique. El servicio debe cubrir igualmente la operación sobre el portal unificado de seguridad de Microsoft y la integración operativa con el SOC como servicio, la plataforma de observabilidad de la ENTIDAD y la herramienta ITSM institucional.

Así mismo, si durante la ejecución del contrato la ENTIDAD adquiere, licencia, habilita, activa o incorpora nuevas herramientas, módulos, funcionalidades o capacidades de seguridad de Microsoft en su tenant o en sus componentes híbridos asociados, el PROVEEDOR debe asumir, sin solución de continuidad, la administración, operación, gestión, integración, soporte, monitoreo, afinamiento, documentación y mejora continua de dichas herramientas o capacidades, en las mismas condiciones de servicio, gobierno, trazabilidad e integración previstas en el presente numeral y sus subnumerales, siempre que correspondan al objeto contractual.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

La incorporación de nuevas herramientas o capacidades deberá formalizarse mediante el procedimiento de gestión de cambios, con actualización del inventario, alcance, línea base, responsabilidades, esfuerzo operativo y, cuando corresponda, aplicación de los precios unitarios o mecanismos económicos establecidos en el contrato.

Las referencias a Microsoft y a sus productos corresponden a herramientas actualmente licenciadas, habilitadas o implementadas en la ENTIDAD, cuya administración constituye el objeto específico del servicio S23. Estas referencias no se extienden como condición de marca a los demás servicios del proceso.

Documentación: Plan de servicio, inventario de herramientas/capacidades bajo administración, arquitectura objetivo y arquitectura de integración aprobada, incluyendo actualizaciones del inventario y del alcance cuando se incorporen nuevas herramientas o capacidades.

S23.2. Modalidad del servicio

El servicio debe incluir: (i) operación del día a día (BAU), (ii) administración y cambios (configuración/hardening), (iii) gestión de incidentes y respuesta en coordinación con SOC, (iv) mejora continua (casos de uso, ajustes de políticas, optimización) y (v) soporte y transferencia de conocimiento.

Documentación: Catálogo de servicios + RACI + plan de transición.

Gobierno, operación y gestión del servicio

S23.3. Gobierno y RACI

El PROVEEDOR debe definir y operar un modelo de gobierno con roles y responsabilidades (RACI) para: administración de Microsoft Entra ID, Microsoft Purview, Microsoft Sentinel, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, Microsoft Defender for Cloud, capacidades premium de Microsoft Intune y demás herramientas/capacidades de seguridad Microsoft activas en la ENTIDAD; gestión de cambios; incidentes; problemas; requerimientos; y reporting, articulado con el SOC como servicio y con el ITSM institucional. En caso de incorporación de nuevas herramientas, módulos o capacidades de seguridad de Microsoft durante la ejecución contractual, el PROVEEDOR debe actualizar el modelo de gobierno, el RACI, los procedimientos, los runbooks, los playbooks, el inventario y los flujos de integración para incluirlas dentro de la operación del servicio.

Documentación: Matriz RACI + acta de socialización.

S23.4. Operación del portal unificado de seguridad

El PROVEEDOR debe administrar y operar de manera centralizada el portal unificado de seguridad de Microsoft y los componentes de seguridad que en él converjan, garantizando consistencia de

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

parametrización, segregación de funciones, control de acceso, trazabilidad de acciones administrativas, correlación entre incidentes y conservación de evidencia técnica.

Documentación: Procedimiento operativo del portal, matriz de roles/RBAC, bitácora de administración y reporte de auditoría.

S23.5. Plan de transición y estabilización

El PROVEEDOR debe ejecutar un plan de transición que incluya: levantamiento de estado, línea base, riesgos, backlog priorizado, victorias tempranas (quick-wins) y estabilización.

Documentación: Informe de diagnóstico + backlog priorizado + plan de trabajo.

S23.6. Gestión de cambios

El PROVEEDOR debe gestionar cambios mediante ITSM institucional, incluyendo evaluación de impacto, plan de reversa, ventana de cambio, evidencia post-cambio y actualización documental (as-built) acorde con el procedimiento de gestión de cambios de la ENTIDAD.

Documentación: Registros de cambio en ITSM + evidencia técnica.

S23.7. Documentación operativa

El PROVEEDOR debe entregar y mantener actualizados: runbooks, playbooks, Procedimiento Operativo Estandar (SOP), diagramas lógicos de integración y guía de operación por componente/capacidad.

Documentación: Repositorio documental versionado.

Integraciones obligatorias (SOC + Observabilidad + ITSM)

S23.8. Flujo operativo con SOC

El PROVEEDOR debe integrar la operación de Entra/Purview/Sentinel y demás herramientas de seguridad Microsoft al modelo del SOC como servicio, garantizando: triage, escalamiento, contención, erradicación, recuperación y lecciones aprendidas, con niveles de severidad acordados.

Documentación: Procedimiento de gestión de incidentes + matriz de escalamiento.

S23.9. Normalización y trazabilidad de eventos/incidentes

El PROVEEDOR debe asegurar que los eventos/alertas/incidentes gestionados cuenten, como mínimo, con: ID único, severidad, fecha/hora, origen, activo/identidad afectada, correlación, estado, responsable y evidencia asociada; y que esos campos se conserven en integraciones hacia SOC/ITSM/observabilidad.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Documentación: Especificación de campos + muestra de registros exportados.

S23.10. Automatización y orquestación

El PROVEEDOR debe implementar/administrar automatizaciones (reglas y flujos) para enriquecer, notificar, crear tickets y ejecutar acciones de respuesta, según lineamientos del SOC y aprobaciones de la ENTIDAD.
Documentación: Catálogo de automatizaciones + bitácora de ejecución.

S23.11. Telemetría operativa

El PROVEEDOR debe integrar a la herramienta de observabilidad institucional métricas/estados de operación (salud de conectores, fallos de ingesta, latencias, errores de automatización, disponibilidad, estado de sensores, salud de sincronización, fallos de políticas y eventos críticos), usando mecanismos soportados por la ENTIDAD.
Documentación: Dashboards y alertas en observabilidad + guía de operación.

S23.12. Alertamiento proactivo

El PROVEEDOR debe configurar alertas proactivas para degradación del servicio (caída de conectores, disminución de ingesta, fallos de políticas, errores de auditoría, degradación de sensores o fallos en componentes híbridos) y canalizarlas a ITSM/SOC según criticidad.
Documentación: Reglas de alerta + evidencias de disparo controlado.

S23.13. Gestión integral en ITSM

El PROVEEDOR debe operar incidentes, requerimientos, problemas y cambios a través de ITSM institucional, incluyendo: categorización, prioridad, SLA, asignación, evidencias y cierre con causa raíz cuando aplique.
Documentación: Tickets en ITSM con trazabilidad.

S23.14. CMDB / Elementos de Configuración (CIs)

El PROVEEDOR debe relacionar tickets con CIs/activos de CMDB (identidades, aplicaciones, repositorios, recursos cloud, componentes híbridos, sensores, conectores, certificados, políticas y demás elementos administrados) y proponer actualizaciones de CMDB cuando identifique brechas de inventario.
Documentación: Tickets vinculados a CIs + reporte de hallazgos CMDB.

Requerimientos técnicos por componente/capacidad administrada
Microsoft Entra (identidad y acceso)

S23.15. Gobierno de identidades y acceso

El PROVEEDOR debe administrar y optimizar políticas y configuraciones de identidad y acceso (MFA, Restablecimiento de Contraseña de Autoservicio (SSPR), acceso condicional, protección

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

de identidad y controles de sesión), alineadas con el modelo de riesgo institucional.
Documentación: Matriz de políticas + configuración exportable + acta de aprobación.

S23.16. Identidad híbrida y servicios de directorio

El PROVEEDOR debe administrar y fortalecer los controles de identidad híbrida de la ENTIDAD, incluyendo la relación operativa entre Microsoft Entra ID y Directorio Activo (AD), la salud de conectores, sincronización, dependencias, políticas de acceso, hardening y la operación de sensores, agentes o componentes requeridos por las herramientas de seguridad asociadas a identidad.
Documentación: Inventario de componentes híbridos, diagrama lógico actualizado, matriz de dependencias y reporte de salud de sincronización/sensores.

S23.17. Privilegios y cuentas administrativas

El PROVEEDOR debe administrar controles para cuentas privilegiadas (mínimo privilegio, activación bajo aprobación, trazabilidad, revisiones periódicas) y mantener bitácoras de actividad administrativa. Incluye capacidades de gestión de privilegios como PIM cuando aplique.
Documentación: Procedimiento + reportes de actividad privilegiada.

S23.18. Gobierno de identidades y riesgos

El PROVEEDOR debe administrar y operar las capacidades de protección de identidad, gobierno y verificación que se encuentren licenciadas/activas en la ENTIDAD, incluyendo, cuando aplique, revisiones de acceso, automatización del ciclo de vida de identidad/acceso, controles sobre acceso privilegiado, acceso temporal aprobado, verificación reforzada de identidad y demás capacidades disponibles en la familia Microsoft Entra.
Documentación: Matriz de políticas, evidencias de revisiones de acceso, reportes de aprobaciones/revocaciones y bitácoras de actividad privilegiada.

S23.19. Ciclo de vida y revisiones

El PROVEEDOR debe operar revisiones periódicas de accesos y membresías críticas, con evidencia de recertificación y remediación (altas/bajas/cambios), articulado con ITSM.
Documentación: Reporte de revisiones + tickets de remediación.

Microsoft Purview (cumplimiento, protección de información y datos)

S23.20. Clasificación y etiquetado

El PROVEEDOR debe administrar el esquema de clasificación/etiquetado (sensibilidad, retención cuando aplique y controles asociados), garantizando versionado, pruebas y despliegue controlado.
Documentación: Catálogo de etiquetas + evidencia de publicación.

S23.21. DLP y controles de exfiltración

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

El PROVEEDOR debe configurar y operar políticas DLP para ubicaciones, canales y repositorios definidos por la ENTIDAD, con modo prueba, umbrales, excepciones justificadas, gestión de alertas y afinamiento (tuning).
Documentación: Inventario de políticas DLP + reporte de alertas y ajustes.

S23.22. Seguridad de correo y colaboración

El PROVEEDOR debe administrar y operar las capacidades de seguridad de correo electrónico y colaboración de Microsoft Defender for Office 365, incluyendo como mínimo políticas, alertas, investigación, remediación, afinamiento y la integración de incidentes/alertas y telemetría con Microsoft Sentinel, SOC, observabilidad e ITSM, cuando aplique.
Documentación: Inventario de políticas activas, reporte de alertas/incidentes gestionados, bitácora de afinamiento y evidencias de integración con Sentinel/ITSM.

Nota: Las capacidades descritas en el numeral S23.22 son complementarias al servicio S5 — Seguridad de Correo Electrónico y no constituyen su reemplazo. Ambos servicios deben operar de manera coordinada bajo la supervisión de la ENTIDAD.

S23.23. Detección y respuesta de identidad

El PROVEEDOR debe administrar y operar Microsoft Defender for Identity, incluyendo la supervisión de señales de identidad de entornos on-premises, cloud e híbridos, la salud de sensores, la investigación de alertas, el enriquecimiento de incidentes y la coordinación de acciones de contención y remediación con SOC, Microsoft Entra ID, Directorio Activo e ITSM.
Documentación: Inventario de sensores/componentes, tablero de salud, reporte de alertas y casos gestionados con trazabilidad de remediación.

S23.24. Seguridad de aplicaciones en la nube y CASB

El PROVEEDOR debe administrar y operar Microsoft Defender for Cloud Apps, incluyendo, cuando aplique, descubrimiento de Shadow IT, inventario y evaluación de riesgo de aplicaciones, controles de sesión, alertamiento sobre comportamiento anómalo, políticas de protección de datos e integración con DLP, SOC, observabilidad e ITSM.
Documentación: Catálogo de aplicaciones descubiertas/gestionadas, matriz de riesgo, políticas activas, alertas operadas y registros de acciones ejecutadas.

S23.25. Auditoría, eDiscovery y evidencia digital

El PROVEEDOR debe garantizar la operación y disponibilidad de capacidades de auditoría y soporte a requerimientos de investigación/descubrimiento según procedimientos institucionales, preservando cadena de custodia documental definida por la ENTIDAD. Incluye soluciones de auditoría y eDiscovery disponibles

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

en Purview cuando aplique. Documentación: Procedimientos + reportes de auditoría + registro de solicitudes.

Microsoft Sentinel (SIEM/SOAR y casos de uso)

S23.26. Conectores e ingesta

El PROVEEDOR debe administrar conectores/fuentes definidas por la ENTIDAD, asegurando continuidad de ingesta, normalización y monitoreo de fallos, con alertas a observabilidad/ITSM. Documentación: Inventario de conectores + tablero de salud + evidencias de ingesta.

S23.27. Correlación y operación unificada XDR

El PROVEEDOR debe administrar la operación unificada de incidentes, alertas, entidades y hunting entre las herramientas de la familia Microsoft Defender y Microsoft Sentinel, garantizando consistencia de clasificación, enriquecimiento, correlación, deduplicación, priorización y trazabilidad de acciones de respuesta. Documentación: Procedimiento XDR/SIEM, matriz de correlación, catálogo de automatizaciones y muestra de incidentes con trazabilidad extremo a extremo.

S23.28. Gestión de exposición, vulnerabilidades y remediación

El PROVEEDOR debe administrar y operar Microsoft Defender Vulnerability Management o las capacidades equivalentes habilitadas en el portal de seguridad de Microsoft para descubrimiento continuo de activos, evaluación de vulnerabilidades y configuraciones, priorización basada en riesgo, seguimiento de remediación y medición de reducción de exposición. Documentación: Inventario de activos, reporte de hallazgos priorizados, plan de remediación, tickets ITSM y tablero de seguimiento.

S23.29. Seguridad de nube, postura y cargas de trabajo

El PROVEEDOR debe administrar y operar Microsoft Defender for Cloud sobre los recursos cloud, híbridos y multicloud definidos por la ENTIDAD, incluyendo postura de seguridad, recomendaciones, alertas, protección de cargas de trabajo, integración con flujos de investigación y remediación, y coordinación con el SOC para la gestión de incidentes. Documentación: Inventario de recursos bajo cobertura, tablero de postura, recomendaciones, alertas e incidentes con su correspondiente trazabilidad.

S23.30. Administración avanzada de dispositivos y privilegios

El PROVEEDOR debe administrar y operar las capacidades premium de Microsoft Intune que se encuentren habilitadas/licenciadas/activas en la ENTIDAD, incluyendo como mínimo, cuando aplique, Endpoint Privilege Management, Remote Help y Cloud PKI, así como otras capacidades avanzadas de soporte, privilegios, certificados, analítica

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		y gestión avanzada disponibles en la suscripción de la ENTIDAD. Estas capacidades deben operar con enfoque de mínimo privilegio, trazabilidad, evidencias de auditoría e integración con Microsoft Entra ID, SOC, observabilidad e ITSM. Documentación: Inventario de capacidades activas, políticas, reportes de sesiones/ayuda, eventos de elevación, bitácoras y evidencias de operación. S23.31. Acceso seguro centrado en identidad Cuando la ENTIDAD tenga habilitadas/licenciadas capacidades de Microsoft Entra Internet Access o Microsoft Entra Private Access, el PROVEEDOR debe administrarlas y operarlas dentro del servicio, incluyendo políticas de acceso, publicación y protección de recursos, segmentación lógica, trazabilidad, monitoreo e integración con SOC, observabilidad e ITSM. Documentación: Políticas activas, matriz de acceso, reportes de operación, alertas y evidencias de integración. S23.32. Casos de uso, correlación y reglas El PROVEEDOR debe diseñar, ajustar y operar casos de uso (detecciones, correlaciones, analíticas) priorizados por riesgo, con ciclo de vida: diseño → prueba → despliegue → afinamiento (tuning) → revisión periódica. Documentación: Backlog de casos de uso + documentación por regla. S23.33. Gestión de incidentes y playbooks El PROVEEDOR debe configurar flujos de incidentes, automatizaciones y playbooks para enriquecimiento, contención y coordinación con SOC/ITSM, manteniendo control de cambios y segregación de funciones. Documentación: Catálogo de playbooks + bitácora de ejecución + tickets. S23.34. Cacería de Amenazas y reportes (Threat hunting y reporting) El PROVEEDOR debe ejecutar ejercicios de hunting según plan acordado y entregar reportes con hallazgos, recomendaciones y acciones de remediación trazadas en ITSM. Documentación: Informes de hunting + tickets asociados. S23.35. Hunting multidominio El PROVEEDOR debe ejecutar hunting y análisis proactivo sobre telemetría de identidad, correo y colaboración, aplicaciones SaaS y nube, utilizando las capacidades disponibles en Microsoft Defender y Microsoft Sentinel, y debe registrar hallazgos, hipótesis, indicadores, recomendaciones y acciones de remediación en ITSM. Documentación: Informes de hunting, consultas o artefactos equivalentes, tickets asociados y plan de remediación. Nota de integración: Cuando aplique, el PROVEEDOR debe soportar integraciones entre Purview y Sentinel mediante los mecanismos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

disponibles en dichas soluciones, así como entre Sentinel y las soluciones de la familia Microsoft Defender habilitadas en el tenant.

Seguridad de la operación del servicio (controles del PROVEEDOR)

S23.36. Acceso de terceros y segregación

El PROVEEDOR debe operar bajo mínimo privilegio, segregación de funciones y acceso administrado; todo acceso administrativo debe quedar auditado y ser trazable a una identidad individual. Documentación: Matriz de accesos + reportes de auditoría.

S23.37. Gestión de credenciales y secretos

El PROVEEDOR debe custodiar secretos/credenciales conforme a políticas institucionales y controles equivalentes, sin exposición en texto plano ni repositorios no autorizados. Documentación: Procedimiento + evidencias de bóveda/gestión de secretos.

S23.38. Confidencialidad y tratamiento de información

El PROVEEDOR debe cumplir acuerdos de confidencialidad y restricciones de tratamiento de datos definidos por la ENTIDAD, garantizando que la información institucional no se use para fines distintos al objeto contractual. Documentación: Compromisos firmados + controles operativos.

Niveles de servicio (SLA/SLO) y métricas (KPI)

S23.39. SLAs

El PROVEEDOR debe proponer y cumplir SLAs mínimos para: (i) atención de incidentes por severidad, (ii) tiempos de resolución/restauración, (iii) tiempos de atención de requerimientos, (iv) tiempos de implementación de cambios estándar y (v) comunicación/escalamiento.
Documentación: Matriz SLA + reportes mensuales de cumplimiento. Los valores de referencia definitivos se establecen en el Catálogo ANS FGN, definido en el Anexo Técnico 5 — Acuerdo de Niveles de Servicio (ANS). La medición oficial es responsabilidad exclusiva de la plataforma de Observabilidad/ITSM institucional FGN.

S23.40. KPIs

El PROVEEDOR debe medir y reportar, como mínimo: disponibilidad operacional, salud de conectores, volumen de incidentes por severidad, MTTD/MTTR (si aplica), tasa de falsos positivos, cumplimiento de cambios, backlog y envejecimiento de tickets, y nivel de automatización. Documentación: Tablero + informe mensual.

Los indicadores definitivos se definen en el Catálogo ANS FGN (Anexo Técnico 5 — Acuerdo de Niveles de Servicio). La medición y reporte oficial se realiza a través de la plataforma de Observabilidad/ITSM institucional FGN.

S23.41. KPIs específicos por capacidad

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Además de los KPIs generales del servicio, el PROVEEDOR debe medir y reportar, cuando aplique:
a) salud de sensores y cobertura de identidades híbridas;
b) volumen y criticidad de alertas de correo y colaboración;
c) aplicaciones SaaS descubiertas, categorizadas y con control aplicado;
d) activos con exposición/vulnerabilidades priorizadas;
e) recursos cloud con hallazgos de postura o workload protection;
f) ejecuciones de privilegio elevadas, sesiones de soporte remoto y certificados administrados;
g) automatizaciones ejecutadas y efectividad de correlación XDR/SIEM.
Documentación: Tablero e informe mensual con datos fuente verificables.

Perfiles mínimos y experiencia

S23.42. Equipo mínimo

El PROVEEDOR debe asignar un equipo con experiencia demostrable en administración/operación de herramientas de seguridad Microsoft (incluyendo Entra, Purview, Sentinel, Defender for Office 365, Defender for Identity, Defender for Cloud Apps, Defender for Cloud y capacidades premium de Intune, cuando apliquen) e integración con SOC/ITSM/observabilidad, de acuerdo con los perfiles establecidos en el ANEXO TÉCNICO 6 PERFILES PROFESIONALES.

Reportes (operativos, ejecutivos y de mejora)

S23.43. Reportes operativos periódicos

El PROVEEDOR debe generar y entregar reportes operativos con información verificable de la operación de las herramientas de seguridad de Microsoft y de sus integraciones con SOC, observabilidad e ITSM. Los reportes deben reflejar la totalidad de herramientas y capacidades de seguridad Microsoft bajo administración, incluyendo aquellas incorporadas, habilitadas, activadas o licenciadas durante la ejecución del contrato, con su respectiva trazabilidad de entrada en operación.
Documentación: Reporte(s) en repositorio definido por la ENTIDAD y/o tickets ITSM asociados.

S23.44. Contenido mínimo de reportes

Los reportes deben incluir como mínimo: (i) estado de salud de conectores, sensores, ingesta y automatizaciones; (ii) indicadores SLA/KPI; (iii) principales incidentes/casos por herramienta y su correlación en el portal unificado; (iv) cambios ejecutados con plan de reversa y evidencias; (v) afinamiento/tuning y reducción de ruido; (vi) hallazgos de exposición/vulnerabilidades y remediación; (vii) riesgos y backlog priorizado; y (viii) recomendaciones de mejora continua.
Documentación: Reporte con anexos de evidencias (exportables, capturas autorizadas, logs, IDs en ITSM/observabilidad/SOC).

Criterios y pruebas de aceptación (FAT/SAT/operativas)

S23.45. Plan de pruebas de aceptación

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		El PROVEEDOR debe definir, acordar y ejecutar un plan de pruebas de aceptación para: (i) puesta en operación inicial, (ii) aceptación de integraciones SOC—observabilidad—ITSM, y (iii) aceptación de cambios relevantes (nuevos conectores, reglas, políticas, sensores, automatizaciones y componentes híbridos). Documentación: Plan de pruebas con casos, precondiciones, datos de prueba, responsables, criterios de éxito y evidencias de ejecución. S23.46. Criterios mínimos de aceptación Para dar por aceptado el servicio y sus entregables, como mínimo debe verificarse: a) integración ITSM: creación/actualización/cierre de tickets desde eventos/incidentes, cuando aplique, con campos mínimos y trazabilidad; b) integración Observabilidad: dashboards/alertas operativas con umbrales y notificación probada; c) integración SOC: flujo de escalamiento y manejo de severidades probado con evidencia; d) trazabilidad: cada incidente/cambio debe tener ID y evidencia asociada; e) operación y trazabilidad sobre el portal unificado de seguridad Microsoft; f) cobertura efectiva de las herramientas/licencias activas incluidas en el alcance; g) salud operativa de sensores, conectores, agentes y dependencias; h) disponibilidad de reportes operativos y ejecutivos con datos consistentes. Documentación: Evidencias por caso de prueba (IDs, capturas autorizadas, exportables, logs). S23.47. Pruebas de aceptación de integraciones El PROVEEDOR debe ejecutar pruebas controladas de: (i) ingesta de logs/telemetría, (ii) correlación/creación de incidente, (iii) automatización (enriquecimiento/notificación/ticket), y (iv) visualización/alertamiento en observabilidad; documentando resultados. Documentación: Registro de ejecución de pruebas y resultados, con evidencias adjuntas. S23.48. Matriz Requisito—Evidencia—Aceptación El PROVEEDOR debe mantener una matriz de aceptación que relacione: requisito (S23.x), documentación producida, caso de prueba ejecutado, resultado y estado de aceptación. Documentación: Matriz actualizada y versionada. Plan de salida (exit plan / reversibilidad / transferencia) S23.49. Plan de salida y reversibilidad El PROVEEDOR debe entregar y mantener actualizado un plan de salida aplicable a finalización, terminación anticipada o cambio de proveedor, que garantice continuidad operativa y reversibilidad sin pérdida de trazabilidad documental. Documentación: Documento “Plan de salida” aprobado, con

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		cronograma, responsables, RACI y checklist de actividades. S23.50. Entregables obligatorios de salida El plan de salida debe contemplar como mínimo: a) transferencia de conocimiento; b) entrega de documentación operativa vigente; c) entrega de inventarios (conectores, reglas, políticas, sensores, automatizaciones y configuraciones exportables cuando aplique), incluyendo las herramientas, módulos, funcionalidades o capacidades de seguridad de Microsoft que se hayan incorporado, habilitado, activado o licenciado durante la ejecución del contrato; d) entrega del histórico de reportes y matriz de aceptación; e) revocación ordenada de accesos del PROVEEDOR y evidencias de auditoría; f) entrega de backlog/riesgos y estado de tickets en ITSM; g) confirmación de eliminación/retención de información del PROVEEDOR conforme a lineamientos de la ENTIDAD. Documentación: Checklist de salida diligenciado + acta de entrega/recibo. S23.51. Prueba de salida El PROVEEDOR debe ejecutar una validación final que demuestre: (i) continuidad del monitoreo/alertamiento, (ii) trazabilidad de tickets y reportes, (iii) accesos del PROVEEDOR revocados sin afectación del servicio, y (iv) documentación/inventarios entregados. Documentación: Resultados de validación y evidencias.
Empaque y rotulado	N/A	
Presentación y Unidad de Medida	N/A	

Concepto	Nombre y apellidos	Rol	Firma
Aprobó	Giselle Viviana Muñeton Lara	Coordinador	GISELLE VIVIANA MUÑETON LARA Firmado electrónicamente por Giselle Viviana Muñeton Lara Fecha: 2026.11.06 14:19:46 -05'00'
Elaboró	Nelson Javier Castelblanco Avila	Estructurador	NELSON JAVIER CASTELBLANCO AVILA Firmado electrónicamente por NELSON JAVIER CASTELBLANCO AVILA Fecha: 2026.11.06 11:57:56 -05'00'
Elaboró	Leonardo Barreto Florez	Estructurador	LEONARDO BARRETO FLOREZ Firmado electrónicamente por LEONARDO BARRETO FLOREZ Fecha: 2026.11.06 12:06:46 -05'00'
Elaboró	Emerson Cruz Aldana	Estructurador	EMERSON CRUZ ALDANA Firmado electrónicamente por EMERSON CRUZ ALDANA Fecha: 2026.11.06 12:40:05 -05'00'
Revisó	Eric Mauricio Vargas Forero	Jefe de Infraestructura TI	ERIC M VARGAS FORERO Firmado electrónicamente por ERIC M VARGAS FORERO Fecha: 2026.11.06 14:07:39 -05'00'

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Revisó	Joan Andres Perdomo Hernandez	Estructurador	JOAN ANDRES PERDOMO HERNANDEZ Firmado electrónicamente por JOAN ANDRES PERDOMO HERNANDEZ Fecha: 2026.11.06 13:57:12 -05'00'
Revisó	Jose Luis Daza Perez	Estructurador	JOSE LUIS DAZA PÉREZ Firmado electrónicamente por Jose Luis Daza Pérez Fecha: 2026.11.06 13:48:20 -05'00'

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada