DOCUMENTO DE CARACTERIZACIÓN DE LA NECESIDAD

1. IDENTIFICACIÓN, DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD

1.1. ANTECEDENTES

La Empresa Nacional Promotora del Desarrollo Territorial S.A.-, de conformidad con lo previsto en el artículo 1.2.2.1. del Decreto 1082 de 2015, tiene por objeto principal ser agente en cualquiera de las etapas del ciclo de proyectos de desarrollo, mediante la preparación, financiación y administración de estudios, y la preparación, financiación, administración y ejecución de proyectos, principalmente aquellos incluidos en los objetivos del Plan de Desarrollo, convirtiéndose en un socio estratégico para el Gobierno Nacional y un articulador del desarrollo económico regional.

La Empresa Nacional Promotora del Desarrollo Territorial S.A..- es una Entidad al servicio del Estado para agenciar las políticas de desarrollo del Gobierno Nacional y de los niveles territoriales, mediante la financiación, administración, estructuración y promoción de proyectos en todos los sectores, a través de las siguientes líneas de negocios: a) Estructuración de Proyectos; b) Gerencia de Proyectos - Gerencia de Proyectos con Recursos Internacionales; c) Gestión de Proyectos; y d) Evaluación de Proyectos.

De conformidad con lo establecido en los Artículos 13 y 15 de la Ley 1150 de 2007, el régimen jurídico de contratación de ENTerritorio S.A. es el del derecho privado. Por lo tanto, las normas que regulan sus contratos serán el Código Civil, el Código de Comercio, las disposiciones del Estatuto Orgánico del Sistema Financiero y las demás disposiciones especiales que le sean aplicables en consideración a su naturaleza jurídica.

El régimen aplicable a cada contrato que ENTerritorio S.A. celebre se determinará de acuerdo con la posición contractual que ostente. Así, cuando funja como parte contratista se sujetará al régimen jurídico aplicable al contratante; y cuando actúe en calidad de contratante se regirá por el derecho privado, en concordancia con lo dispuesto por los artículos 13 y 15 de la Ley 1150 de 2007.

Dentro de la organización y estructura de ENTerritorio S.A., se encuentra El Grupo de Tecnologías de la Información dependencia adscrita a la Gerencia General, la cual tiene asignadas entre otras las siguientes funciones[1]: *"1. Diseñar, asesorar, impulsar y poner en marcha las estrategias para la debida implementación y el mejoramiento continuo de la gestión estratégica de las tecnologías de la información y las comunicaciones que contribuyan al logro de los objetivos misionales de ENTerritorio, bajo las directrices dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, o el que haga sus veces. (…) 4. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de ENTerritorio en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia. (…) 13. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio, con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en ENTerritorio. (…) 15. Liderar el desarrollo, implementación y mantenimiento de los sistemas de información y servicios digitales de ENTerritorio en virtud de lo establecido en el Plan Estratégico de Tecnologías de la*

[1] Numeral 1.4 Tecnologías de la Información de la Resolución No. 137 del 31 de mayo de 2023 *"Por la cual se determinan los grupos de trabajo de la Empresa Nacional Promotora del Desarrollo Territorial - ENTerritorio y se establecen sus funciones"*.

Información y de las comunicaciones, así como también, las necesidades de información de los servicios al ciudadano y grupos de interés. (…) 16. Liderar la definición y supervisión de las capacidades de infraestructura tecnológica, servicios de administración, operación y soporte y velar por la prestación eficiente de los servicios tecnológicos necesarios para garantizar la operación de los sistemas de información y servicios digitales según criterios de calidad, oportunidad, seguridad, escalabilidad y disponibilidad. (…) 21. Establecer los lineamientos institucionales para el uso óptimo de los recursos tecnológicos con que cuenta la Entidad. (…) 22. Definir y documentar la metodología para el desarrollo, prueba, puesta en producción, mantenimiento y continuidad de los sistemas de información de la Entidad (…)".

Conforme a lo establecido en el Manual de Políticas de Seguridad de la Información M-RI-06 Versión 3, Numeral 12.6 Gestión De Vulnerabilidad Técnica específicamente el subnumeral 12.6.1 Gestión de las vulnerabilidades técnicas, indica: "(…) Se debe realizar una adecuada gestión de los riesgos relacionados con la seguridad de la información, teniendo en cuenta que éstos se identifican con base en las vulnerabilidades presentadas en los activos de información y las amenazas que podrían aprovechar dichas vulnerabilidades. II. El Grupo de Tecnologías de la Información por sus propios medios o por medio de un tercero, realizará tres (3) análisis de vulnerabilidades al año de la infraestructura tecnológica de la entidad. III. Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, y en general sobre la infraestructura tecnológica de la Entidad, evaluar la exposición de esta ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados. Este proceso de diagnóstico será liderado por el equipo de Ciberseguridad. IV. El Grupo de Tecnologías de la Información debe participar en la definición de los planes de tratamiento para mitigar los riesgos y realizar la remediación de las vulnerabilidades en seguridad informática, identificadas en la infraestructura tecnológica. Así mismo, incluirá la revisión del avance de los mencionados planes dentro de sus actividades de monitoreo al cumplimiento de lineamientos de seguridad de la información. V. La metodología para la identificación y valoración de los riesgos en Seguridad de la Información, así como para la formulación de tratamientos para mitigarlos, está integrada con la metodología del Sistema de Administración del Riesgo Operativo, con el fin de contar con una visión integral de los riesgos. Dicha metodología está descrita en el manual M-RI-03 Manual de Gestión de Riesgos Operacionales y en los procedimientos asociados. VI. El equipo de Ciberseguridad debe efectuar, por lo menos una vez al año, procesos de análisis de vulnerabilidades sobre los activos de información, infraestructura tecnológica y física que los soporta, y comportamiento de administradores y usuarios finales en relación con la seguridad de la información (pruebas de ingeniería social), cuyos resultados, una vez analizados, deben actuar como insumo para la actualización del perfil de riesgo en seguridad de la información. Estos procesos pueden llevarse a cabo por colaboradores del grupo o a través de contratos con empresas especializadas. (…).".

Con el objetivo de asegurar la integridad, confidencialidad y disponibilidad de la información gestionada por la Empresa Nacional Promotora del Desarrollo Territorial (ENTerritorio S.A.), se han desarrollado diversas iniciativas y proyectos en el ámbito de la seguridad de la información. Estos esfuerzos responden a la necesidad de cumplir con las normativas y regulaciones establecidas por el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), así como a la creciente importancia de proteger los activos de información frente a un panorama de amenazas en constante evolución.

El marco normativo que rige la seguridad de la información en Colombia incluye el Decreto 1078 de 2015, el cual expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicacio-

nes. Este decreto, en su Título 9, Políticas y Lineamientos de Tecnologías de la Información, Capítulo 1, Estrategia de Gobierno en Línea (GEL), define los componentes de seguridad y privacidad de la información como elementos esenciales de la estrategia de Gobierno en Línea.

Posteriormente, el Decreto 1008 de 2018 establece los lineamientos generales de la política de Gobierno Digital, subrogando el capítulo 1 del título 9 del Decreto 1078 de 2015. Este decreto introduce la Política de Gobierno Digital, que incluye habilitadores transversales como la Arquitectura Empresarial, la Seguridad y Privacidad, y los Servicios Ciudadanos Digitales. Estas normativas enfatizan la importancia de implementar medidas de seguridad robustas en todos los procesos, trámites, servicios y sistemas de información.

La Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones establece los lineamientos y estándares para la estrategia de seguridad digital, adoptando el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. Esta resolución, en su Artículo 17, numeral 2, subnumeral 1.5, requiere la realización periódica de auditorías de seguridad de la información, tanto para aspectos de gestión como técnicos, incluyendo análisis de vulnerabilidades y pruebas de penetración.

La Resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones establece los lineamientos y estándares para la protección de datos personales en la relación con proveedores, adoptando un enfoque integral de seguridad y privacidad para asegurar la confidencialidad, integridad y disponibilidad de la información. Esta resolución, en su Artículo 12, numeral 3, subnumeral 2.1, requiere que todas las entidades públicas y privadas que manejan datos personales implementen medidas de seguridad adecuadas para proteger dicha información durante todo el ciclo de vida del dato, desde su recolección hasta su eliminación.

Además, la Superintendencia Financiera ha establecido, en la Parte I, Título II, Capítulo 1 de la Circular Básica Jurídica, los lineamientos que deben seguir las entidades públicas respecto a los canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros. Esto incluye la protección de los criterios de confidencialidad, disponibilidad e integridad de la información. En cumplimiento de estos lineamientos, ENTerritorio S.A. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos del estándar ISO/IEC 27001:2013.

En el marco del Plan Estratégico de Tecnologías de Información (PETI) 2024-2027 de ENTerritorio S.A., se han definido proyectos clave para fortalecer la seguridad informática de la entidad. El PETI es una hoja de ruta esencial que guía la implementación y desarrollo de tecnologías de información, alineando los objetivos tecnológicos con las metas estratégicas de la organización. Entre los proyectos más relevantes se encuentran:

- PROY13: Orientado al fortalecimiento de los controles de seguridad informática, este proyecto busca mejorar las defensas contra amenazas cibernéticas y garantizar la protección de los sistemas y datos críticos de la entidad.
- PROY10: Destinado a robustecer los controles de seguridad para los activos en la nube publica de ENTerritorio S.A., asegurando una gestión efectiva de los riesgos de ciberseguridad y la protección de la reputación institucional.

Estos proyectos están alineados con los objetivos estratégicos y operativos de ENTerritorio S.A., asegurando una infraestructura tecnológica segura y resiliente. El PETI 2024-2027 establece metas claras y medibles para

mejorar la seguridad de la información, incluyendo la implementación de nuevas tecnologías, el fortalecimiento de las capacidades de respuesta a incidentes y la mejora continua de los procesos de seguridad.

Para cumplir con las normativas y objetivos estratégicos establecidos, es necesario contratar soluciones de seguridad específicas que permitan una protección integral y continua de los activos de información de ENTerritorio S.A. Estas soluciones incluyen plataformas de firewall de próxima generación en la nube y Sandbox Integral

La implementación de estas soluciones garantizará la protección efectiva contra amenazas, permitirá una gestión proactiva y eficiente de la seguridad de la información y asegurará la continuidad y resiliencia operativa de ENTerritorio S.A. Estas inversiones son estratégicas para mantener y mejorar la seguridad de la información, alineándose con el Plan Estratégico de Tecnologías de Información (PETI) 2024-2027 y contribuyendo al cumplimiento de los estándares normativos y regulatorios establecidos.

El objeto a contratar se encuentra incluido dentro del Plan Anual de Adquisiciones mediante el código No 1491.

1.2. JUSTIFICACIÓN Y DESCRIPCIÓN DE LA NECESIDAD DE LA CONTRATACIÓN

Con el fin de dar cumplimiento a lo establecido por el Ministerio de Tecnologías de la Información y Comunicaciones MINTIC a través del Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” que en su Título 9, Políticas Y Lineamientos De Tecnologías De La Información, Capitulo 1, Estrategia de Gobierno en Une - GEL, en la SECCION 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES, se define el compone e de seguridad y privacidad de la información, como parte integral de la estrategia de Gobierno en Línea, la Empresa Nacional Promotora del Desarrollo Territorial - ENTerritorio S.A., en cabeza del Grupo de Planeación y Gestión del Riesgo, ha desarrollado actividades de identificación y mitigación de posibles escenarios de riesgo para la seguridad de la información, una de estas actividades es la identificación de vulnerabilidades en sus diferentes sistemas de información de manera ágil y oportuna,

El Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, dentro de su Título 9, se encarga de definir las políticas y lineamientos de las tecnologías de la información, y los instrumentos y plazos de la Estrategia GEL.

El Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", define componentes, habilitadores, y fines de la Política de Gobierno Digital. Es decir, el Estado Colombiano está actualmente en un proceso de transformación de una Estrategia de Gobierno en Línea a una Política de Gobierno Digital, la cual en los términos del citado decreto se compone entre otros de Habilitadores transversales, “Elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales” como lo son:

- Arquitectura Empresarial: Busca el fortalecimiento de las capacidades institucionales y de gestión de TI.

- Seguridad y Privacidad: Busca implementar los lineamientos de seguridad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general.

- Servicios Ciudadanos Digitales: Prestación de los servicios ciudadanos digitales para permitir el acceso a la administración pública a través de medios electrónicos.

La Resolución 500 de 2021 del Ministerio de las Tecnologías de la Información “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, en su Artículo 17, numeral 2. Protección y Detección, subnumeral 1.5, establece la realización periódica de auditorías de seguridad de la información tanto para los aspectos de gestión como para los aspectos técnicos, incluyendo auditorías internas y externas al modelo de Seguridad y Privacidad de la Información, análisis de vulnerabilidades, hacking ético, pruebas de penetración a sistemas informáticos y pruebas de ingeniería social, entre otras.

Así mismo, la Superintendencia estableció en la Parte I, Título II, Capítulo 1 de la Circular Básica Jurídica, los lineamientos que debe aplicar ENTerritorio S.A. respecto a los canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros, específicamente con relación a la protección de los criterios de confidencialidad, disponibilidad e integridad de la información gestionada en la Entidad. De esta manera, las Entidades públicas de orden nacional y las entidades públicas del orden territorial tienen la obligatoriedad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), el cual comprende, entre otros requisitos, la identificación y gestión de los riesgos relacionados con la seguridad de la información institucional y la planeación e implementación de los controles, según lo establecido en el Anexo A del estándar ISO/IEC 27001:2013 de seguridad de la información.

Considerando la necesidad de cumplir con los estándares normativos y de seguridad, es imprescindible la contratación de soluciones específicas que permitan una protección integral y continua de los activos de información de ENTerritorio S.A. Estas soluciones incluyen la implementación de:

- NGFW Cloud: Esta solución ofrece una plataforma de firewall de próxima generación en la nube, proporcionando capacidades avanzadas de firewall, reconocimiento de aplicaciones y control granular. Estas funcionalidades son esenciales para prevenir accesos no autorizados y proteger las aplicaciones críticas de la entidad contra amenazas externas e internas.

- Sandbox Integral: La solución de sandboxing es vital para analizar y detectar archivos y comportamientos sospechosos en un entorno controlado, sin riesgo para los sistemas reales. Este análisis avanzado permite identificar amenazas sofisticadas y desconocidas que podrían eludir las defensas tradicionales, fortaleciendo así la seguridad de la infraestructura de nube publica de azure de ENTerritorio S.A.

- Tecnología de engaño: La tecnología de engaño (Deception Technology) proporciona una capa adicional de defensa mediante la creación de señuelos y trampas para detectar, desviar y responder a actividades maliciosas dentro de la red. Esta solución implementa activos falsos que simulan recursos críticos, atrayendo a los atacantes y permitiendo su detección temprana. Al identificar y analizar las tácticas de los atacantes en estos entornos controlados,

Estas soluciones de seguridad son cruciales para cumplir con los requerimientos legales y regulatorios establecidos, así como para garantizar la protección de la confidencialidad, disponibilidad e integridad de la información gestionada por ENTerritorio S.A. Además, estas herramientas permitirán a la entidad adelantarse a

las amenazas, gestionar vulnerabilidades de manera efectiva y mantener la continuidad operativa. La implementación de estas soluciones contribuirá significativamente a la confianza y seguridad de los servicios prestados a la ciudadanía y otras partes interesadas, fortaleciendo la postura de seguridad de la entidad y asegurando el cumplimiento del Manual de Políticas de Seguridad de la Información M-RI-06 Versión 3, Numeral 12.6 Gestión de Vulnerabilidad Técnica, específicamente el subnumeral 12.6.1 Gestión de las vulnerabilidades técnicas.

Adicionalmente, esta necesidad está claramente descrita en el Plan Estratégico de Tecnologías de Información (PETI) de ENTerritorio S.A. para el período 2024-2027. El PETI es una hoja de ruta fundamental que guía la implementación y desarrollo de tecnologías de información dentro de la entidad, alineando los objetivos tecnológicos con las metas estratégicas de la organización. En este plan, se detallan proyectos específicos orientados al fortalecimiento de la seguridad informática de la entidad. Por ejemplo, el proyecto identificado como PROY13, que se enfoca en el fortalecimiento de los controles de seguridad informática, y el proyecto PROY10, destinado a robustecer los controles de seguridad para los activos en la nube pública. Ambos proyectos están alineados con los objetivos estratégicos y operativos de ENTerritorio S.A., asegurando una infraestructura tecnológica segura y resiliente.

El PETI 2024-2027 establece metas claras y medibles para mejorar la seguridad de la información, incluyendo la implementación de nuevas tecnologías, el fortalecimiento de las capacidades de respuesta a incidentes y la mejora continua de los procesos de seguridad. Este plan no solo responde a las necesidades actuales de seguridad, sino que también se anticipa a futuros desafíos, asegurando que ENTerritorio S.A. esté bien equipada para enfrentar un panorama de amenazas en constante evolución. La alineación de los proyectos de seguridad con el PETI garantiza que las inversiones en tecnologías de información sean estratégicas, efectivas y contribuyan al logro de los objetivos generales de la organización.

En resumen, la contratación de estas soluciones es una medida estratégica y necesaria para mantener y mejorar la seguridad de la información en ENTerritorio S.A., asegurando así el cumplimiento normativo y la protección de los activos de información frente a un panorama de amenazas en constante evolución. Estas inversiones no solo garantizarán la protección efectiva contra posibles amenazas, sino que también permitirán una gestión proactiva y eficiente de la seguridad de la información, asegurando la continuidad y resiliencia operativa de la entidad.

2. OBJETO Y ALCANCE

2.1. OBJETO

La Empresa Nacional Promotora del Desarrollo Territorial ENTerritorio S.A., está interesada en contratar la “La adquisición, implementación, mantenimiento de soluciones avanzadas, incluidos los servicios de soluciones integrales avanzadas de seguridad informática para nube publica para ENTerritorio S.A.”

2.2. ALCANCE DEL OBJETO

- NGFW Cloud (Cantidad: 1): Plataforma de firewall de próxima generación en la nube, esencial para prevenir accesos no autorizados y proteger las aplicaciones críticas, por un período de tres (3) años contados a partir de su activación.

- Sandbox Integral (Cantidad: 1): Solución de sandboxing para analizar y detectar comportamientos sospechosos en un entorno controlado, por un período de tres (3) años contados a partir de su activación.
- Solución de tecnología de Deception para el cambio de las defensas de reactivas a proactivas con detección basada en la intrusión, en capas con la inteligencia contextual, por un período de tres (3) años contados a partir de su activación.
- Soporte y mantenimiento: Servicio integral que incluye, asistencia técnica, apoyo en la administración, y resolución de incidencias para asegurar el funcionamiento óptimo de todas las soluciones contratadas (NGFW, Sandbox y Deception), garantizando la disponibilidad y seguridad del entorno durante un período de doce (12) meses contados a partir de la activación de las soluciones NGFW Cloud, Sandbox Integral y Solución de tecnología de Deception.

2.2.1. DEFINICIÓN DE LAS ESPECIFICACIONES O DESCRIPCIÓN TÉCNICA DETALLADA Y COMPLETA DEL BIEN, OBRA O SERVICIO A CONTRATAR

2.2.1.1. Solucion NGFW Cloud VM

Item	NGFW Cloud VM
1.1	La solución debe consistir en una plataforma de protección de red basada en un dispositivo virtual con funcionalidades de Firewall de Próxima Generación (NGFW), estando aprobado para ser provisionado en al menos las siguientes Nubes Públicas: Amazon (AWS), Azure (Microsoft), OCI (Oracle) y GCP (Google).
1.2	La funcionalidad NGFW significa: Firewall, reconocimiento de aplicaciones, IPS/IDS, identificación de usuarios y control granular de permisos;
1.3	Todos los recursos demandados en este término deberán permanecer operativos y actualizados durante la vigencia del contrato;
1.4	Debe usar maximo 8 vCPU
1.5	Debe soportar maximo 2 TB
1.6	Debe soportar maximo 500 dominios de virtualizacion
1.7	Debe soportar minimo 200.000 politicas de firewall
1.8	Debe soportar minimo c6i.2xlarge / c7gn.2xlarge (AWS) o Standard_D8s_v5 (Azure) o n2-standard-8 / t2a-standard-8 (GPC) o VM.Standard3.Flex(4 OCPU) / VM.Standard.A1.Flex (8 OCPU) (Oracle Cloud)
1.9	La gestión de la solución debe soportar el acceso vía SSH, cliente WEB (HTTPS) y API abierta;
1.10	Para la gestión, debe haber una opción para configurar las redes de origen permitidas para el acceso remoto;
1.11	Debe admitir BGP, OSPF, RIP y enrutamiento estático; si se requiere una licencia por separado para cualquier enrutamiento, debe entregarse sin ninguna restricción;
1.12	Debe ser compatible con la traducción de puertos (PAT);
1.13	Debe admitir NAT estático (1 a 1);
1.14	Debe admitir NAT estática bidireccional 1 a 1;
1.15	Debe admitir NAT dinámico (muchos a muchos);

1.16	Debe ser compatible con Source NAT;
1.17	Debe admitir NAT de destino;
1.18	Debe admitir NAT de origen y NAT de destino simultáneamente;
1.19	Debe implementar la traducción de prefijos de red (NPTv6) o NAT66, evitando problemas de enrutamiento asimétrico;
1.20	Debe ser compatible con NAT64;
1.21	Debe permitir monitorear vía SNMP el uso de CPU, memoria, espacio en disco, VPN, situación del clúster y violaciones de seguridad;
1.22	Debe permitir el envío de logs a sistemas de gestión externos;
1.23	Debe haber una opción para enviar registros a sistemas de gestión externos en forma encriptada, a través del protocolo SSL;
1.24	Debe tener mecanismos de protección contra la suplantación de identidad;
1.25	Debe ser compatible con la operación de Capa 3 (L3), para la inspección de datos en línea y la visibilidad del tráfico;
1.26	Debe tener una calificación de nivel AAA en Cyber Ratings (organismo de investigación independiente) para la categoría Cloud Network Firewall;
1.27	Debe tener control SSL, inspección y descifrado para el tráfico saliente;
1.28	Debe admitir la integración nativa con los proveedores más reconocidos de certificado, para obtener automáticamente certificados válidos
1.29	Debe tener funciones de automatización, para facilitar la operación diaria de los firewalls. Apoyar, al menos, la realización de acciones como ejecutar scripts, enviar correos electrónicos, notificaciones a través de Teams y API a través de hosts comprometidos, programación, cambios de configuración y la ocurrencia de eventos de red y seguridad predefinidos;
1.30	Debe incluir conectores para funciones de SASE y SDWAN
2	**Características generales**
2.1	Debe admitir la operación en el modelo Hub&Spoke en todas las nubes compatibles mencionadas en el punto 1.1
2.2	Admite configuración de alta disponibilidad Activa/Pasiva y Activa/Activa;
2.3	Debe admitir el modelo de alta disponibilidad con cada miembro del clúster aprovisionado en una zona de nube pública separada;
2.4	Debe ser compatible con el modelo de alta disponibilidad activo-pasivo mediante el equilibrador de carga nativo de la nube pública
2.7	Debe admitir la escala vertical (aumentar el tamaño de la VM en uso) en la nube pública
3	**Modos de operación**
3.1	Debe soportar controles por zonas de seguridad;
3.2	Soportará controles de política por puerto y protocolo;
3.3	Soportará controles de políticas por aplicaciones, grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones;
3.4	Debe permitir Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad;
3.5	Debe permitir el control de políticas por país (por ejemplo: Brasil, Estados Unidos, Reino Unido, China);

3.6	Debe permitir el control, la inspección y el descifrado de SSL por política para el tráfico saliente;
3.7	Debe permitir descifrar el tráfico saliente en conexiones negociadas con TLS 1.2 y TLS 1.3;
3.8	Debe permitir el bloqueo de archivos por su extensión y permitir la correcta identificación del archivo por su tipo incluso cuando se cambie el nombre de su extensión;
3.9	Debe admitir objetos y reglas de IPV6;
3.10	Debe soportar la asignación de horarios preestablecidos para el funcionamiento de las políticas, con el objetivo de habilitar y deshabilitar automáticamente las políticas en horarios predefinidos;
3.11	Debe tener una opción de aprovisionamiento y configuración inicial de NGFW en una solución SaaS
3.12	Debe permitir la creación de reglas basadas en objetos dinámicos de proveedores de la nube, tales como: Grupo de seguridad, Etiquetas, Instancia, Tipo de instancia, VPC, Subred, Zona de disponibilidad
3.13.1	Los dispositivos de protección de red deben tener la capacidad de reconocer aplicaciones, independientemente del puerto y el protocolo;
3.13.2	Debe ser posible liberar y bloquear solo aplicaciones sin necesidad de liberar puertos y protocolos;
3.13.3	Reconocer al menos 2000 aplicaciones diferentes, incluidas, entre otras: tráfico relacionado entre pares, redes sociales, acceso remoto, actualización de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, archivos para compartir datos, correo electrónico;
3.13.4	Debe inspeccionar la carga útil del paquete de datos para detectar firmas de aplicaciones conocidas por el fabricante, independientemente del puerto y el protocolo;
3.13.5	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de visualizar y controlar aplicaciones y ataques que utilizan tácticas evasivas a través de comunicaciones encriptadas, como Skype y uso de la red Tor;
3.13.6	Para el tráfico cifrado SSL, los paquetes deben descifrarse para poder leer la carga útil para verificar las firmas de las aplicaciones conocidas por el fabricante;
3.13.7	Debe realizar la decodificación del protocolo para detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde a la especificación del protocolo. La decodificación de protocolos también debe identificar una funcionalidad específica dentro de una aplicación;
3.13.8	Identificar el uso de tácticas evasivas a través de comunicaciones encriptadas;
3.13.9	Actualice la base de firmas de la aplicación automáticamente;
3.13.10	Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con integración a Microsoft Active Directory, sin necesidad de instalar un agente en el Controlador de Dominio, o en las estaciones de los usuarios;
3.13.11	Debe ser posible agregar el control de aplicaciones en reglas de seguridad de múltiples dispositivos, es decir, no limitarse solo a la posibilidad de habilitar el control de aplicaciones en algunas reglas;
3.13.12	Debe admitir varios métodos de identificación y clasificación de aplicaciones, al menos mediante la verificación de firmas y protocolos de decodificación;
3.13.13	Permitir de forma nativa la creación de firmas personalizadas para el reconocimiento de aplicaciones propietarias en la interfaz gráfica de la solución, sin necesidad de intervención del fabricante;

3.13.14	El fabricante debe permitir solicitudes para incluir aplicaciones en la base de firmas de aplicaciones;
3.13.15	Debe alertar al usuario cuando una aplicación está bloqueada;
3.13.16	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, emule, etc.) teniendo granularidad de control/políticas para los mismos;
3.13.17	Debe habilitar la diferenciación del tráfico de Mensajería Instantánea (AIM, Hangouts, Facebook Chat, etc.) teniendo granularidad de control/políticas para los mismos;
3.13.18	Debería permitir diferenciar y controlar partes de las aplicaciones, como permitir YouTube y, al mismo tiempo, bloquear la transmisión HD;
3.13.19	Debe permitir la diferenciación de aplicaciones de Proxies (psiphon, freegate, etc.) teniendo granularidad de control/políticas para ellos;
3.13.20	Debería ser posible crear grupos dinámicos de aplicaciones en función de las características de las aplicaciones, tales como: tecnología utilizada en las aplicaciones (cliente-servidor, basado en exploración, protocolo de red, etc.);
3.13.21	Debería ser posible crear grupos dinámicos de aplicaciones en función de las características de la aplicación, como: nivel de riesgo de la aplicación, tecnología, proveedor y popularidad;
3.13.22	Debería ser posible crear grupos estáticos de aplicaciones en función de las características de la aplicación, como: categoría de la aplicación;
3.13.23	Debería permitir forzar el uso de puertos específicos para ciertas aplicaciones;
3.13.24	Debe permitir el filtrado de videos que se pueden ver en YouTube;
3.14.1	Le permite especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
3.14.2	Debe ser posible crear políticas por grupos de usuarios, IPs, redes o zonas de seguridad;
3.14.3	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué URL a través de la integración con los servicios de directorio, Active Directory y la base de datos local;
3.14.4	La identificación por base de Active Directory debería permitir SSO, por lo que los usuarios no necesitan volver a iniciar sesión en la red para navegar a través del firewall;
3.14.5	Debe tener la capacidad de crear políticas basadas en el control por URL y categoría de URL;
3.14.6	Debe tener categorías de URLs previamente definidas por el fabricante y constantemente actualizadas;
3.14.7	Debe tener al menos 60 categorías de URL;
3.14.8	Debe tener la función de excluir URL del bloqueo;
3.14.9	Debe permitir la personalización de la página de bloqueo;
3.14.10	Debe permitir restringir el acceso a canales específicos de YouTube, pudiendo configurar una lista de canales liberados o una lista de canales bloqueados;
3.14.11	Debe permitir bloquear el acceso a contenidos indebidos al utilizar la búsqueda en sitios como Google, Bing y Yahoo, independientemente de que la opción Búsqueda Segura esté habilitada en el navegador del usuario;
3.15.1	Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué aplicaciones a través de la integración con servicios de directorio, autenticación a través de LDAP, Active Directory, E-directory y base de datos local;
3.15.2	Debe tener integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo granularidad de control/políticas basadas en usuarios y grupos de usuarios;

3.15.3	Debe tener integración con Microsoft Active Directory y soporte para el sistema operativo Windows Server 2012 R2 o superior;
3.15.4	Debe tener integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo granularidad de control/políticas basadas en usuarios y grupos de usuarios, soportando single sign-on. Esta funcionalidad no debe tener límites de usuarios con licencia;
3.15.5	Debe tener integración con Radius para identificar usuarios y grupos que permitan granularidad de control/políticas basadas en usuarios y grupos de usuarios;
3.15.6	Debe tener integración con LDAP para identificar usuarios y grupos que permitan granularidad de control/políticas basadas en Usuarios y Grupos de Usuarios;
3.15.7	Debe soportar la identificación de múltiples usuarios conectados a la misma dirección IP en ambientes Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que se encuentran en estos servicios;
3.15.8	Debe admitir el envío y la recepción de credenciales a través de RADIUS;
3.15.9	Debe soportar SAML como método de autenticación en la navegación por Internet y para VPN;
3.16.1	Permitir identificar y, opcionalmente, impedir la transferencia de varios tipos de archivos (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
3.16.2	Admite la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
3.16.3	Permitir identificar y, opcionalmente, evitar la transferencia de información confidencial, incluido, entre otros, el número de tarjeta de crédito, lo que permite la creación de nuevos tipos de datos a través de expresiones regulares.
3.17.1	Apoyar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de un determinado País/Países;
3.17.2	Debe habilitar la visualización de los países de origen y destino en los logs de acceso;
4	**Características del cortafuegos:**
4.1	Para proteger el entorno contra ataques, los dispositivos de protección deben contar con un módulo IPS, Antivirus y Anti-Spyware integrado en el propio sistema operativo NGFW;
4.2	Debe incluir firmas de prevención de intrusiones (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);
4.3	Debe sincronizar firmas IPS, Antivirus, Anti-Spyware cuando se implementa en alta disponibilidad;
4.4	Debe implementar los siguientes tipos de acciones para amenazas detectadas por el IPS: permitir, permitir y registrar, bloquear y poner en cuarentena la IP del atacante por un intervalo de tiempo;
4.5	Las firmas deben poder activarse o desactivarse, o incluso habilitarse solo en modo de monitoreo;
4.6	Debe ser posible crear políticas por usuarios, grupos de usuarios, IPs, redes o zonas de seguridad;
4.7	Las excepciones por IP de origen o de destino deben ser posibles en reglas o firma;
4.8	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
4.9	Debe permitir el bloqueo de vulnerabilidades;
4.10	Debe permitir el bloqueo de exploits conocidos;

4.11	Debe incluir protección contra ataques de denegación de servicio;
4.12	Ser inmune y capaz de prevenir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
4.13	Detectar y bloquear la fuente de escaneos de puertos;
4.14	Bloquear ataques realizados por gusanos conocidos;
4.15	Tener firmas específicas para mitigar los ataques DoS y DDoS;
4.16	Tener firmas para bloquear ataques de desbordamiento de búfer;
4.17	Debe permitir la creación de firmas personalizadas a través de la interfaz gráfica del producto;
4.18	Debe permitir el uso de operadores de negación en la creación de firmas IPS o anti-spyware personalizadas, permitiendo la creación de excepciones con granularidad en las configuraciones;
4.19	Permitir el bloqueo de virus y spyware en, al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;
4.20	Identificar y bloquear la comunicación con botnets;
4.21	Registrar en la consola de monitoreo la siguiente información sobre amenazas identificadas: el nombre de la firma o ataque, aplicación, usuario, origen y destino de la comunicación, además de la acción realizada por el dispositivo;
4.22	Debe tener la función de proteger la resolución de direcciones vía DNS, identificando solicitudes de resolución de nombres para dominios maliciosos de botnets conocidos;
4.23	Los eventos deben identificar el país de donde se originó la amenaza;
4.24	Debe incluir protección contra virus en contenido HTML y javascript, spyware (spyware) y gusanos;
4.25	Contar con protección contra descargas involuntarias mediante HTTP de archivos ejecutables y maliciosos;
4.26	Debe ser posible configurar diferentes políticas de control de amenazas y ataques en base a políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración de IPS diferente, siendo estas políticas por Usuarios. , Grupos de usuarios, origen, destino, zonas de seguridad.
4.27	Debe ser capaz de mitigar amenazas persistentes avanzadas (APT), a través de análisis dinámicos para identificar malware desconocido;
4.28	Entre los análisis realizados, la solución debe soportar antivirus, consulta en la nube, emulación de código, sandboxing y verificación de devolución de llamada;
4.29	La solución debe permitir el envío de archivos sospechosos para análisis de comportamiento en un ambiente controlado;
4.30	Debe permitir la integración con fuentes de amenazas externas: admite al menos listas de IP, hash de malware y dominios;
5	**Funciones de seguridad**
5.1	Debe poseer y tener licencia para la funcionalidad VPN IPSec de sitio a sitio;
5.2	Debe poseer y tener licencia de la funcionalidad VPN de cliente a sitio de IPSec;
5.3	Debe tener y tener licencia de la funcionalidad VPN de acceso telefónico IPSec, en caso de que el extremo remoto no tenga una IP estática en la WAN;
5.4	La VPN IPSEC debe ser compatible con el cifrado 3DES, AES128, AES192 y AES256 (Advanced Encryption Standard);
5.5	IPSEc VPN debe admitir autenticación MD5, SHA1, SHA256, SHA384 y SHA512;

5.6	IPSEc VPN debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14, Grupo 15 a 21 y Grupo 27 a 32;
5.7	IPSEc VPN debe ser compatible con el algoritmo de intercambio de claves de Internet (IKEv1 y v2);
5.8	IPSEc VPN debe admitir la autenticación a través del certificado IKE PKI;
5.9	Debe soportar el uso de DDNS, para los casos en que uno o ambos extremos tengan IPs dinámicas;
5.10	La función DDNS debe admitir tanto IPv4 como IPv6;
5.11	Debe tener y tener licencia para la funcionalidad SSL VPN;
5.12	La funcionalidad VPN SSL debe permitir su uso con y sin cliente VPN, es decir, apoyar al usuario a realizar la conexión a través de un cliente VPN instalado en el equipo o a través de un navegador Web (sin cliente VPN instalado en el equipo);
5.13	Debe permitir que todo el tráfico de los usuarios remotos de VPN fluya hacia el túnel VPN, evitando la comunicación directa con dispositivos locales como proxies, etc.;
5.14	Debe permitir que los usuarios remotos reenvíen al túnel VPN solo el tráfico corporativo configurado por los administradores, y que todo el tráfico no seleccionado sea manejado por la red local del usuario remoto;
5.15	Debe permitir la asignación de DNS en clientes VPN remotos, incluso con DNS de túnel dividido;
5.16	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antipyware y filtrado de URL para el tráfico de clientes remotos conectados a la VPN SSL;
5.17	Debe admitir autenticación a través de AD/LDAP, certificado y base de usuarios local;
5.18	Debe soportar lectura y verificación de CRL (lista de revocación de certificados);
5.19	Debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL VPN;
5.20	La VPN SSL debe permitir que los usuarios remotos cambien las contraseñas en Active Directory;
5.21	SSL VPN debe permitir la personalización de pantalla en sesiones RDP;
5.22	El firewall debe permitir que se configure como un cliente VPN SSL, lo que permite que el tráfico de los usuarios locales se canalice a través de esta VPN;
5.23	El agente VPN SSL o IPSEC de cliente a sitio debe ser compatible con al menos: Windows 7 (32 y 64 bits), Windows 8.1 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10. 14 y superior);
6	**Funciones de conectividad**
6.1	La solución debe proporcionar recursos de enrutamiento inteligente, definiendo, a través de reglas preestablecidas, el mejor camino a seguir para una aplicación;
6.2	Debe habilitar la terminación de túneles VPN establecidos por soluciones "on-premise", así como realizar enrutamiento inteligente entre nubes públicas;
6.3	Debería ser posible crear políticas que definan los siguientes criterios para que coincidan: direcciones de origen; Grupos de Usuarios; direcciones de destino; DSCP; Aplicación de capa 7 utilizada (O365 Exchange, AWS, Dropbox, etc.);

6.4	La solución debe ser capaz de monitorear e identificar fallas a través de la asociación de chequeo de salud, permitiendo pruebas de respuesta por ping, http, tcp/udp echo, dns, tcp-connect y twamp;
6.5	SD-WAN debe equilibrar el tráfico de aplicaciones a través de múltiples enlaces simultáneamente;
6.6	La SD-WAN debe analizar el tráfico en tiempo real y balancear los paquetes de un mismo flujo (sesión) entre múltiples enlaces simultáneamente;
6.7	Se debe permitir la creación de políticas de enrutamiento basadas en los siguientes criterios: latencia, jitter, pérdida de paquetes, ancho de banda ocupado o todo al mismo tiempo;
6.8	La solución SD-WAN debe permitir el uso de túneles VPN dinámicos, entre extremos remotos, para aplicaciones confidenciales. Una vez que los puntos finales intercambian información entre sí, se establece un túnel directo entre los puntos finales y se omite el concentrador;
6.9	Debe permitir la duplicación de paquetes entre dos o más enlaces, de forma selectiva, buscando una mejor experiencia de uso de las aplicaciones empresariales;
6.10	La solución debe permitir definir el enrutamiento para cada aplicación;
6.11	Deben estar presentes varias formas de elegir el enlace, incluyendo: el mejor enlace, el costo más bajo y la definición de los niveles mínimos de calidad que se aceptarán para que dichos enlaces puedan usarse en un enrutamiento de aplicación dado;
6.12	Debería permitir definir el enlace de salida para una aplicación específica;
6.13	Debe implementar el equilibrio de enlaces por hash de IP de origen;
6.14	Debe implementar el equilibrio de enlace de hash de IP de origen y destino;
6.15	Debe implementar el equilibrio ponderado de enlaces. En esta opción debería ser posible definir el porcentaje de tráfico que será drenado por cada uno de los enlaces.
6.16	Debe implementar balanceo de enlaces sin la obligación de crear zonas o usar instancias virtuales;
6.17	La solución SD-WAN debe ser compatible con el enrutamiento basado en políticas o el reenvío basado en políticas;
6.18	Para IPv4, debe admitir enrutamiento estático y dinámico (BGP y OSPF);
6.19	Debe contar con un recurso de corrección de errores (FEC), que permita reducir las pérdidas de paquetes en las transmisiones. La solución debe realizar ajustes dinámicos en la relación de pérdida de paquetes x envío de paquetes redundantes;
6.20	Debe ser posible habilitar FEC para tráfico específico. Ej: solo para aplicaciones sensibles a la pérdida de paquetes;
6.21	Debe permitir la personalización de los temporizadores para detectar fallas en el enlace, así como el tiempo necesario para que el enlace vuelva a equilibrarse después del restablecimiento;
6.22	La solución SD-WAN debe admitir de forma nativa conectores con nubes públicas. Al menos: Azure, AWS, GCP y OCI;
6.23	Debe permitir la creación de reglas basadas en objetos dinámicos, tales como: instancias, imagen, nombre, ID de subred y etiqueta;
6.24	Para poder controlar las aplicaciones y el tráfico cuyo consumo pueda ser excesivo (como YouTube, Facebook, etc.), impactando en el buen uso de las aplicaciones empresariales, se requiere que la solución, además de poder permitir o denegar este tipo de aplicación, debe tener la capacidad de controlarlos dando forma a las políticas. Entre los posibles tratamientos, la solución debe incluir:

6.25	Admite la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, usuario y grupo de usuarios, aplicaciones y puerto;
6.26	La QoS debe permitir la definición de tráfico con ancho de banda garantizado. Ej: ancho de banda mínimo disponible para aplicaciones comerciales;
6.27	La QoS debe permitir la definición de tráfico con el máximo ancho de banda. Ej.: ancho de banda máximo permitido para aplicaciones de mejor esfuerzo/no corporativas, como Youtube, Facebook, etc.;
6.28	También debe habilitar el marcado DSCP, para que esta información pueda usarse a lo largo de la red troncal con fines de reserva de ancho de banda;
6.29	La QoS debe permitir la definición de una cola de prioridad;
6.30	Además de permitir la definición de ancho de banda máximo y garantizado por aplicación, también debe admitir coincidencias en categorías de URL, IP de origen y destino, inicios de sesión y puertos;
6.31	La capacidad de programar intervalos de tiempo en los que las políticas de modelado/QoS serán válidas es obligatoria. Ej.: regla de control de ancho de banda más permisiva durante las horas de almuerzo;
6.32	Debe permitir la definición de diferentes bandas para descargar y cargar;
6.33	La solución SD-WAN debe proporcionar estadísticas en tiempo real sobre la ocupación del ancho de banda (carga y descarga) y el rendimiento de la verificación de estado (pérdida de paquetes, inestabilidad y latencia);
6.34	La solución SD-WAN debe admitir la verificación de estado activa, pasiva y mixta:
6.35	Activo: creación manual de chequeo de salud, definiendo el destino a medir y el protocolo;
6.36	Pasivo: uso de tráfico real para mediciones;
6.37	Mixto: Pasivo cuando hay tráfico de usuarios y, en su ausencia, cambio al método activo;
6.38	La solución SD-WAN debe ser compatible con IPv6;
6.39	Debe habilitar un enrutamiento distinto según el grupo de usuarios seleccionado en la regla SD-WAN;
6.40	La SD-WAN debe tener un servicio Stateful Firewall;
6.41	La solución SD-WAN debe proporcionar cifrado AES de 128 bits o AES de 256 bits en su VPN;
6.42	Se espera que la solución SD-WAN simplifique la implementación de túneles encriptados de sitio a sitio;
6.43	Debe poder bloquear el acceso a las aplicaciones;
6.44	Debe admitir NAT dinámico y NAT de salida;
6.45	Debe admitir el equilibrio de tráfico por sesión y de paquetes;
6.46	La solución SD-WAN se puede proporcionar en combinación con el firewall, siempre que cumpla con los mismos requisitos de rendimiento;
7	**Funciones de interoperabilidad**
7.1	Debe tener conectores nativos para la integración con nubes privadas, al menos: VMware ESXI, Cisco ACI y Kubernetes;
7.2	Debe tener conectores nativos para la integración con nubes públicas, al menos: AWS EKS, Azure AKS, GCP Kubernetes, Oracle Kubernetes.

7.3	Debe ser compatible con la automatización para responder a eventos de seguridad, con soporte para la integración con AWS Lambda, Azure Function, Google Cloud Function para el flujo de trabajo
7.4	La solucion de NFGW y Sandbox deben ser del mismo fabricante para realizar una rapida respuesta ante eventos de seguridad.

2.2.1.2. Solución de Sandbox integral

Item	**Características del equipamiento de Sandbox integral**
1.0	Se requiere que el oferente incluya los créditos, puntos o licenciamiento BYOL, o lo que considere segun el caso, que permita lograr las siguientes capacidades mínimas y funcionalidades:
1.1	Throughput mínimo en modo sniffer de 1 Gbps.
1.2	Capacidad de procesar al menos 280 archivos por hora en VM de sandbox.
1.3	Capacidad de procesar archivos utilizando prefiltros de sandbox de al menos 7500 archivos por hora.
1.4	Capacidad de procesar archivos en de forma estatica minimo 15000 archivos por hora.
1.6	La solución debe permitir ejecutar al menos 14 VMs simultaneas para sandboxing.
1.7	Incluir la licencia necesaria para utilizar al menos 14 VMs simultaneas.
1.8	Incluir al menos 14 licencias de Microsoft Windows y tres licencias de Microsoft Office.
1.9	La solución debe de ser del tipo Máquina Virtual
2.0	**Requerimientos Mínimos de Funcionalidad**
2.1	La solución debe proporcionar la funcionalidad de inspeccionar el tráfico entrante en busca de malware desconocido (APT - Advanced Persistent Threat y Zero-Day Threats), ransomware con filtrado avanzado de amenazas y análisis de ejecución en tiempo real, e inspección del tráfico saliente. devoluciones de llamada.
2.2	Poseer la capacidad de prevenir amenazas desconocidas.
2.3	Debido a que el malware es muy dinámico y un Antivirus reactivo común no es capaz de detectarlos con la misma velocidad con la que se crean sus variaciones, la solución ofrecida debe contar con funciones de prevención de malware desconocido incluidas en la propia herramienta (zero-day).
2.4	El dispositivo de protección debe poder analizar archivos automáticamente localmente, donde el archivo se ejecutará y simulará en un entorno controlado.
2.5	Debe admitir el monitoreo de archivos traficados en Internet (HTTPs, FTP, HTTP, SMTP), así como archivos traficados internamente entre servidores de archivos usando SMB en todos los modos de implementación: sniffer, transparente y L3.
2.6	La solución debe poder inspeccionar el tráfico cifrado SSL.
2.7	La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
2.8	Seleccionar a través de la política qué tipos de archivos se someterán a este análisis.
2.9	Implementar e identificar la existencia de malware en archivos adjuntos de correo electrónico y URL conocidas.
2.10	La solucion debe estar en capacidad de soportar cluster minimo hasta 80 nodos.
2.11	La solucion debe estar en capacidad de implementarse como PaaS, IaaS, VM u on-prem.

2.12	La solucion de NFGW y Sandbox deben ser del mismo fabricante para realizar una rapida respuesta ante eventos de seguridad.
3.0	**Funcionalidades de ATP**
3.1	Implementar la detección y el bloqueo inmediatos de malware que utiliza mecanismos de escaneo en archivos PDF.
3.2	La solución debe soportar los siguientes sistemas operativos dentro de su entorno controlado: Windows 7, Windows 8.1, Windows 10, Windows 11, MacOS, Android, Linux y sistemas ICS
3.3	Admite el análisis de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en el entorno de sandbox.
3.4	Debe soportar como mínimo los siguientes tipos de Archivos: . .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm,.dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf,.pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx,.swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx,.xz, .z, .zip, odt.
3.5	Los entornos controlados que posee la solución deben tener al menos las siguientes aplicaciones instalados: Internet Explorer, Adobe Flash Player, Adobe Reader, Microsoft .NET Framework, Microsoft Office, Java Runtime y MSVC Runtime
3.6	Debe incluir un módulo de web filtering para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan.
3.7	Al finalizar un análisis, debe poder informar sobre las actividades realizadas durante su ejecución. La mínima información con la que debe contar es: procesos iniciados, archivos creados/modificados/eliminados, cambios realizados en el registro y comportamiento de red.
3.8	Debe permitir al operador interactuar con el sistema operativo de la instancia virtual en entorno controlado mientras se realiza un análisis bajo demanda.
3.9	Debe ser posible descargar un archivo PCAP para revisar el comportamiento del archivo analizado.
3.10	Debe permitir hacer un análisis de los archivos con intervención interactiva del operador sobre la máquina virtual.
3.11	Debe permitir realizar una grabación de video del comportamiento del malware.
3.12	Debe contener mecanismos de cache para evitar múltiples análisis del mismo archivo.
3.13	La solución debe incluir la totalidad del licenciamiento requerido para la ejecución de los ambientes controlados.
3.14	Para el análisis de correo electrónico, debe extraer la URL contenida en el cuerpo o adjunto del mensaje y acceder a la URL, descargar el archivo correspondiente y ejecutarlo en un ambiente controlado
3.15	La solución debe tener una nube de inteligencia propietaria del fabricante que se encargue de actualizar toda la base de seguridad a través de firmas.
3.16	La solución debe admitir topologías de implementación en modo sniffer.
3.17	La solución debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP, BCC o relay SMTP.
3.18	La solución debe admitir topologías de implementación mediante el intercambio de archivos (SMB,NFS).
3.19	La solución debe admitir topologías de implementación bajo demanda, es decir, mediante envío manual a través de la consola gráfica.
3.20	La solución debe admitir topologías de implementación a través de la API JSON.

3.21	La solución debe tener la posibilidad de permitir la carga de máquinas virtuales personalizadas incluyendo sistema operativo y aplicaciones.
3.22	Todo análisis y bloqueo de malware y / o código malicioso debe ocurrir en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y / o códigos maliciosos.
3.33	La solución debe ser compatible con las reglas YARA como estándar para crear reglas para la detección de malware.
3.34	La solucion debe tener por los menos las siguientes tecnicas de deteccion Anti-evasion: • API Obfuscation • Detection Bare-metal • Command and Control • Llamadas directas al sistema • Retardo de Ejecucion • Memory Only Payload • Process Hollowing/Injection • Runtime Encryption/Packing • System Fingerprinting • Time Bomb • Chequeo de archivos de usuario • Chequeo de interaccion de usuario • Deteccion de VM/Sandbox
3.35	Debe soportar Callback detection. Debe evaluar visitas a URL maliciosas, comunicaciones de botnet C&C y trafico de atacante desde Malware activado.
3.36	Debe permitir la integracion con soluciones de correo, syslogs, servidores CEF, SIEM, firewalls, balanceadores, proxy y antivirus por medio de JSON API o ICAP.
3.37	La solucion debe permitir la Emulación sin máquina virtual de códigos ejecutables de Windows (PEXBox) basada en Machine learning.
3.38	Debe estar en capacidad de Detección de amenazas de red en modo sniffer. Identificar actividades de botnets y ataques de red, visitas a URL maliciosas.
3.39	Soporte de escaneo de archivos superiores a 10G
3.4	Soporte de TCP RST para restablecer la conexión con servidores sospechosos
3.41	Debe integrar reglas Yara
4.0	**Funcionalidades de Visibilidad**
4.1	Deberá permitir que el administrador de la solución descargue el archivo original, analizado por la solución sandbox.
4.2	En caso de un veredicto positivo, debe presentar una descripción detallada del comportamiento de la máquina comprometida, que contenga al menos información sobre el tipo de archivo para fines de auditoría.
4.3	En el caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre IP Malware Origin con fines de auditoría.
4.4	En el caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre la IP de destino (cliente que descargó el malware) para fines de auditoría.

4.5	En caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos un resumen del comportamiento del malware con fines de auditoría
4.6	En el caso de archivos identificados como sospechosos, deben poder diferenciarse en al menos tres niveles de riesgo: alto, medio o bajo
4.7	Debe usar herramientas de investigacion y reporteria con base en Mitre Attack v11 minimo
4.8	Debe permitir descargas de rastreo de logs, PCAP e indicadores en formato STIX 2.0
4.9	Debe permitir el escaneo de repositorios de archivos via CIFs, NFS, Buckets de AWS S3 y Azure blob

2.2.1.3. Solución de Deceptor (tecnología de engaño)

ITEM	Características Generales
1	Debe permitir la creación de trampas de alta interacción, con capacidad de clonar activos existentes.
2	El sistema de decepción de amenazas debe poderse integrar con la plataforma de reportería de seguridad y SD-WAN, para generar reportes que contengan al menos: top de ataques por tipo de incidente, top 10 de víctimas por tipo de incidente, top 10 de servicios atacados.
3	La maquina Virtual de decepción debe estar en capacidad de simular Windows 7, Windows 10, Windows 10 (personalizable por BYOL), Windows Server 2016, 2019 y 2022 (personalizable por BYOL), Linux (Ubuntu, CentOS, Redhat), macOS, SSL-VPN Server, Medical (PACS, Infusion pump), POS, ERP, IoT (Router, Switch, Printer and IP-Camera), OT (PLC, HMI, MNG), SAP, SCADA, Outbreak,VOIP (4G/5G), TOMCAT, Webmin, Citrix, ESXi, Elastic-Search, SWIFT.
4	La maquina Virtual de decepción debe estar en capacidad de simularlos servicios de SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, SRTP, MOXA, KAMSTRUP, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, Mysql, MQTT, SIP, XMPP, 3GPP, CANBus, B.BRAUN and VNC.
5	Se deben proporcionar dos (2) máquinas virtuales de deception, cada una con capacidad de crear al menos 20 Señuelos de máquinas virtuales y desplegarse en mínimo 128 Vnets o VPC cada una.
6	Se deben entregar minimo dos (2) licencias para VPC o VLAN o Vnnets para cada máquina de decepcion solicitada.
7	Debe permitir la creación de trampas activas con un flujo de tráfico de red falso entre las trampas implementadas para confundir y desviar a los atacantes que monitorean el tráfico, asegurando que interactúen con las trampas implementadas.
8	Debe realizar ejecución de investigaciones proactivas de los eventos correlacionados para detectar amenazas avanzadas desconocidas.
9	Debe permitir hacer visualización completa del ataque
10	La solución ofertada debe incorporar paquetes de tokens para las máquinas señuelo o VM decoy.
11	La solución ofertada debe soportar las siguientes acciones mediante integración con la solución Perimetral de NGFW. - Bloqueo.

	- Cuarentena. - Exportación de IOCs.
12	La solución deberá proporcionar reportes que caractericen tanto la identificación de incidentes como ataques detectados en la red de la entidad. Estos reportes deben incluir: - Severidad. - Última Actividad. - Tipo del evento. - Información de direccionamiento del atacante. - Información de credenciales de uso del atacante. - Información de direccionamiento de la Victima. - Tiempo de iniciación del ataque - Puertos de ejecución del ataque - Tipo de Ataque - Información de passwords usados por el atacante. - Línea del tiempo. - PCAP del tráfico capturado por el Decoy.
13	Debe estar en capacidad de hacer detección de reconocimientos de red que usen ping (ICMP)
14	Debe contar con señuelos que simulen conectores a base de datos que usend ODBC
15	Debe integrarse con el Firewall de Nueva Generación, de manera que se pueda tener en este último un dashboard centralizado con la información general del dispositivo y los señuelos desplegados.
16	Debe permitir exportar indicadores de compromiso (IOC) al menos en formato CSV para su uso por parte de plataformas externas.
17	Debe permitir el despliegue de señuelos en activos reales para que dirijan al atacante a la solución de Decepción de amenazas.
18	Debe tener la capacidad de emular activos del tipo Gateway de VPN SSL.
19	Debe tener la capacidad de emular activos con servicios SAMBA, SMB, SSH y HTTP/S habilitados.
20	Debe tener la capacidad de definir una lista de Ips legítimas de la red para que no generen alertas cuando interactúen con los señuelos.
21	Debe permitir visualizar en un mapa los señuelos desplegados.
22	Debe tener al menos 4 capas de decepción, con la capacidad de crear los siguientes elementos falsos: - Señuelos de infraestructura (Sistemas operativos, camaras, impresoras, bases de datos, etc). - Carnadas o servicios falsos que se ejecuten sobre los señuelos (servidores web, aplicaciones, etc). - Tráfico de red falso para detectar ataques de tipo MitM o app spoofing, entre otros. - Tokens o recursos falsos desplegados sobre los señuelos (Credenciales, archivos, recursos compartidos, conexiones RDP, etc), Los tokens falsos creados no deben ser visibles para los usuarios de la entidad, únicamente para el atacante. - Todos los elementos falsos se deben despleghar sin requerir instalar agentes sobre la infraestructura real de la entidad
23	La solución se debe poder instalar como appliance virtual y cubrir los siguientes Hipervisores: - VmWare

	- KVM - Hyper-V
24	Debe poder instalarse en infraestructura de nube pública, como mínimo en: - AWS - Azure - Google Cloud Platform
25	Debe escanear automáticamente la red haciendo uso de técnicas de escaneo pasivo y sugerir los elementos de decepción que se deben desplegar.
26	La solución, al desplegar un señuelo, debe permitir una interacción completa sobre el mismo. Esto con el fin de evitar que el atacante detecte que se trata de un señuelo.
27	La solución debe ofrecer diferentes tipos de señuelos para desplegar y adicionalmente, debe permitir la creación de señuelos personalizados.
28	La solución debe soportar el marco de referencia MITRE para Sistemas de Control Industrial (MITRE ICS).
29	Debe estar en la capacidad de crear señuelos falsos del tipo: - SAP - ERP
30	La solución debe tener un motor de inteligencia que emplee técnicas Anti-Reconocimiento y Anti-Exploit para hacer rastreo de atacantes y correlación de campañas en tiempo real.
31	Los indicadores de compromiso generados por la solución se deben poder compartir con diferentes herramientas de seguridad de la entidad. Incluido el formato STIX/TAXII
32	La solución se debe integrar como mínimo con los siguientes elementos: Sistema de NGFW de la entidad Sistema de control de acceso a la red (NAC) de la Entidad Herramienta de Sandbox Solución SIEM Solución de respuesta automática (SOAR) Solución de detección y respuesta en el endpoint (EDR) de la Entidad Virus Total Threat Intelligence
33	Debe ofrecer una representación visual tipo mapa que muestre en tiempo real los ataques o señuelos que han sido tocados por el atacante.
34	Debe poder desplegarse en un entorno fuera de línea, sin acceso a internet.

- Entregables

El contratista deberá suministrar dentro de los diez (10) primeros días calendario contados a partir de la suscripción el acta de inicio los siguientes entregables:

- Cronograma de implementación
- Diagrama de ingeniería de la arquitectura a implementar.
- Plan de migración.
- Documento de la matriz de escalamientos

El contratista deberá suministrar dentro de los sesenta (60) primeros días calendario contados a partir de la suscripción el acta de inicio los siguientes entregables:

- Acta entrega de la evidencia de la activación de la solución tecnológica de acuerdo con las condiciones técnicas requeridas.
- Acceso a la plataforma de capacitación del fabricante para mínimo cuatro (4) personas y transferencia para el líder de proyecto durante la ejecución del contrato.
- Entrega de dispositivos, documentación y realización de actividades asociadas al suministro, instalación, implementación, puesto en marcha y estabilización de la solución

- Acuerdos de Nivel de Servicio.

El contratista debe acompañar de forma permanente y brindar el soporte respectivo a los problemas y tareas de problemas durante al plazo de ejecución del contrato frente a las características técnicas la cual contempla la solución integral, para lo cual se deberá documentar e identificar su causa raíz y error conocido ya sea por correo electrónico o alguna plataforma de tickets del proveedor o de ENTerritorio S.A.S, para lo cual se definieron tiempos mínimos requeridos según su criticidad, estos tiempos podrán adecuarse a los ANS del proveedor siempre y cuando no desmejoren los contenidos en este documento, durante cinco (5) días de la semana las ocho (8) horas del día (5X8), siendo atendido por el personal operativo mínimo requerido del contratista según el grado de atención o prioridad que implique la novedad presentada especificada a continuación:

Novedad en el servicio	Prioridad	Tiempo de Atención
Falla total o bloqueo de la herramienta de seguridad en alguno de sus módulos	Crítica	2 horas
Reporte de fallo en la parametrización y/o recolección de la información	Alta	3 horas
Reporte de fallo en las funcionalidades de los módulos implementados	Media	8 horas
Consulta técnica y/o de uso	Baja	16 horas
Mantenimientos y actualizaciones	Planificada	Planificada
El proceso se deberá llevar a cabo de la siguiente manera: a. La novedad será reportada por parte del(os) supervisor(es) indicando la novedad del servicio, para que de tal modo se resuelva en el tiempo establecido. b. El contratista genera un ticket y se reporta por medio de correo electrónico al personal técnico o funcional a mesadeayuda@enterritorio.gov.co c. El contratista realiza el análisis y diagnóstico de la falla dependiendo de la prioridad.		

d. El contratista pone en marcha los procedimientos para la reparación de la falla, configuración y restablecimiento del servicio afectado, en o antes de los tiempos estipulados según la prioridad presentada en la falla, de igual forma deberá agregar el reporte y documentación de la causa de la falla y la forma de solucionarla.
e. La conexión será de forma segura por VPN u otro medio que ENTerritorio S.A.S proporcionará previamente para dicha labor.

3. DESCRIPCIÓN DE LAS AUTORIZACIONES, PERMISOS Y LICENCIAS PARA LA EJECUCIÓN DEL OBJETO CONTRACTUAL

En caso de requerirse un permiso especial para el desarrollo de alguna de las actividades derivadas de la ejecución del objeto contractual, el contratista se obliga a tramitar y obtener tales permisos, de manera que le permitan cumplir con la normatividad vigente sobre la materia y con el objeto contractual.

4. ANÁLISIS DEL PERSONAL MÍNIMO REQUERIDO PARA LA EJECUCIÓN DEL CONTRATO

No aplica para el presente proceso de contratación.

5. ANÁLISIS DE RIESGOS, MATRIZ DE RIESGOS Y ANÁLISIS DE GARANTÍAS

5.1. ANÁLISIS DE RIESGOS Y MATRIZ DE RIESGOS

Ver documento anexo Formato Anexo Análisis De Riesgos F-PR-32.

5.2. ANÁLISIS DE GARANTÍAS

Ver documento anexo Esquema de Garantías: Formato Anexo Esquema De Garantías F-PR-33

6. PLAZO DE EJECUCIÓN DEL CONTRATO Y SU JUSTIFICACIÓN

El plazo de ejecución del contrato a celebrar será por doce (12) meses, contados a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

6.1. CONDICIÓN RESOLUTORÍA

No aplica para el presente proceso de contratación.

7. LIQUIDACIÓN CONTRACTUAL

De acuerdo con lo dispuesto por el Manual de Contratación ENTerritorio S.A. (M-PR-01, Versión 02), en el Capítulo VIII, numeral 50, 51, 52 y demás disposiciones y normatividad vigentes aplicable a la Entidad el contrato que se suscriba SI requiere ser liquidado.

8. DISPONIBILIDAD PRESUPUESTAL

La Entidad cuenta con la disponibilidad presupuestal de acuerdo con la información que a continuación se relaciona:

Concepto	Rubro	Centro de costo	Centro contable	Fuente	Línea de negocio
Suscripciones vigencia actual	21110071	001700 – Tecnologías de la Información	ENTerritorio S.A. – ENTerritorio S.A.	111 – Empresa Nacional Promotora del Desarrollo Territorial ENTerritorio S.A.	01 – Funcionamiento

9. LUGAR DE EJECUCIÓN

Las actividades requeridas para el cumplimiento del objeto contractual se realizarán de forma presencial en las instalaciones de ENTerritorio S.A., en la Calle 26 No 13 - 19 ciudad de Bogotá D.C. en la dependencia que designe previamente la supervisión del contrato o cualquier otro lugar físico donde ENTerritorio S.A. cumpla su función pública, y de forma remota en la plataforma Microsoft Teams o la que designe previamente la supervisión del contrato.

10. FORMA DE PAGO

ENTerritorio pagará al contratista el valor total del contrato en UN ÚNICO (1) PAGO, una vez se suscriba con el Grupo de Tecnologías de la Información documento expedido por el fabricante de la solución que acredite la vigencia y titularidad de las suscripciones adquiridas, informe de implementación, documento que acredite la vigencia del soporte y mantenimiento por doce meses contados a partir de la activación de las suscripciones y acta de recibo a satisfacción dentro del cual conste la entrega a satisfacción de las suscripciones y servicios,

10.1. REQUISITOS PARA EL PAGO

El pago y/o el desembolso de recursos relacionados con el contrato quedan sometidos al cumplimiento de los siguientes requisitos:

1. EL CONTRATISTA deberá presentar factura o documento equivalente con lleno de requisitos legales y acta de recibo a satisfacción, antes de las fechas establecidas para el cierre contable de la Entidad.

2. En caso de estar obligado a facturar electrónicamente, se debe seguir el siguiente procedimiento:
   - Enviar la factura al correo facturacionelectronica@enterritorio..gov.co para aprobación del al Grupo de tecnologías de la Información en calidad de supervisor del contrato. Este es el único canal dispuesto por ENTerritorio S.A. para la recepción de la factura electrónica y registro ante la DIAN.
     - La factura electrónica debe contener el XML y la representación gráfica de la factura, con las definiciones de la DIAN y deberá cumplir con los requerimientos contenidos en la Resolución

00042 del 5 de mayo de 2020, así como con los requisitos señalados en el artículo 617 del Estatuto Tributario

- La factura debe enviarse para aceptación únicamente cuando se tenga el recibido a satisfacción del bien o servicio prestado.
- El envío y aceptación de la factura electrónica constituye un requisito previo y necesario para continuar con el proceso de trámite y pago de los bienes y/o servicios contratados por la Entidad.
- Para la validación de la factura, no se requiere el envío de anexos o demás documentos exigidos para el trámite del pago y/o desembolso.
- En el evento en que se rechace la factura, el contratista deberá ajustarla y enviarla nuevamente.

3. El CONTRATISTA acreditará al Gerente del Grupo de Tecnologías de la Información en calidad de supervisor del contrato, el cumplimiento de sus obligaciones frente al Sistema de Seguridad Social Integral y Parafiscales (Cajas de Compensación Familiar, SENA, e ICBF) de conformidad con lo establecido en la normatividad vigente.

4. EL CONTRATISTA deberá presentar Certificado de Cumplimiento para el Pago (Formato F-FI-06) suministrado por ENTerritorio S.A., el cual debe ser aprobado por el Gerente del Grupo de Tecnologías de la Información en calidad de supervisor del contrato.

5. El pago se realizará dentro de los diez (10) días calendario siguientes a la fecha de radicación de la factura y demás documentos antes citados.

6. Toda vez que los impuestos y retenciones que surjan por la celebración y ejecución del contrato corren por cuenta de EL CONTRATISTA, la Empresa Nacional Promotora del Desarrollo Territorial - ENTerritorio S.A. hará las retenciones del caso y cumplirá las obligaciones fiscales que ordene la ley.

7. ENTerritorio S.A. no se hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el Contrato.

10.2. SISTEMA DE PAGO

El sistema de pago del contrato es PRECIOS UNITARIOS FIJOS SIN FORMULA DE REAJUSTE, teniendo en cuenta que para la ejecución del objeto contractual se encuentran establecidas las características técnicas, al igual que los precios unitarios.

ENTerritorio S.A. no reconocerá, por consiguiente, ningún reajuste realizado por el Contratista en relación con los costos, gastos o actividades adicionales que aquel requería para suscripción y ejecución, y que fueron previsibles al momento de la presentación de la oferta.

Por lo anterior, el valor pactado incluye todos los gastos, tasas y contribuciones derivados u originados de la celebración y ejecución del contrato, las deducciones a que haya lugar, la remuneración para el Contratista,

imprevistos, transporte y, en general, todos los costos en los que deba incurrir el Contratista para el cabal cumplimiento de ejecución del contrato.

11. OBLIGACIONES DE LAS PARTES

11.1. OBLIGACIONES GENERALES DEL CONTRATISTA

1. Cumplir con todas y cada una de las condiciones establecidas en los documentos del proceso y en la oferta aceptada por la Entidad.
2. Dar cumplimiento a sus obligaciones frente al Sistema de Seguridad Social Integral y Parafiscales (Cajas de Compensación Familiar, SENA, e ICBF) y ARL de conformidad con lo establecido en la normatividad vigente.
3. Acatar las instrucciones que durante el desarrollo del contrato se le impartan por parte de la Supervisión
4. Informar por escrito a la Supervisión del Contrato, en el caso en que durante el tiempo de ejecución del contrato surja alguna eventualidad de fuerza mayor o caso fortuito que afecte a cualquiera de las partes.
5. Constituir y mantener vigente la (s) Garantía (s) exigida (s), en los términos requeridos.
6. Cargar en la Plataforma del SECOP II de manera oportuna, los documentos requeridos para el perfeccionamiento y ejecución del contrato.
7. Las demás que contribuyan a garantizar el cumplimiento del contrato y las que por su naturaleza le sean atribuibles conforme al objeto y alcance de este.

11.2. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA.

1. Suministrar las soluciones conforme a lo descrito en las especificaciones técnicas por tres (3) años a partir de su activación. Esta deberá ser aprobada por el supervisor del contrato.
2. Realizar la activación de las suscripciones dentro de los diez (10) días hábiles siguientes contados a partir de la suscripción del acta de inicio.
3. Entregar documento que acredite la vigencia de las suscripciones adquiridas a nombre de la Empresa Nacional Promotora del Desarrollo Territorial S.A..
4. Suscribir el acta de recibo a satisfacción correspondiente con el Gerente del Grupo de Tecnologías de la Información
5. Entregar un cronograma dentro los cinco (5) primeros días hábiles, contados a partir de la fecha de suscripción del acta de inicio, el cual debe incluir la entrega, instalación, puesta en marcha de la solución, y las sesiones de transferencia de conocimiento de mínimo cuatro (4) horas para mínimo (4) personas designadas por la supervisión del contrato; así como, el total de las configuraciones requeridas y pruebas de funcionamiento antes de lanzarlo a producción, este cronograma deberá ser aprobado por el supervisor del contrato.
6. Realizar la transferencia de conocimiento para mínimo cuatro (4) personas designadas por la supervisión, dentro del portal del fabricante, con una intensidad horaria mínima de 16 horas, del uso y manejo de las funcionales en temas de administración, monitoreo y resolución de problemas de las plataformas de la solución implementada, dentro del plazo de ejecución del contrato y cronograma aprobado por el supervisor.
7. Realizar la hardenización de los productos adquiridos conforme a las buenas prácticas de seguridad digital.

8. El contratista deberá ajustar y mantener todos los aspectos de seguridad de los equipos siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del proveedor, por los cambios realizados.
9. El contratista deberá alinearse a las políticas de seguridad de la entidad, así como el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las Telecomunicaciones de Colombia – Mintic;
10. Las actividades de instalación, configuración y puesta en producción de la solución deberán ser realizadas por personal certificado por el fabricante.
11. Configurar y revisar los reportes / logs de las plataformas.
12. El contratista deberá entregar junto con la solución ofertada una garantía emitida por el fabricante, por un término no menor a TRES (3) años a partir de su activación; esta deberá incluir un esquema de soporte 7x24, acceso al portal de soporte, recursos técnicos y solicitar soporte por incidentes vía web, chat y teléfono.
13. Realizar la Implementación, configuración y puesta en marcha de la solución ofertada, la cual deberá ser recibida a satisfacción por el supervisor del contrato.
14. Al finalizar la puesta en funcionamiento de la solución, el contratista deberá entregar toda la arquitectura y configuración de solución documentada detalladamente, esta deberá ser aprobada por el supervisor del contrato.
15. El contratista deberá incluir servicio de soporte técnico del nivel 1 y 2 en modalidad 5 días x 8 horas a la semana de la solución ofertada durante doce (12) meses a partir de la activación de las suscripciones.
16. El contratista deberá apoyar al personal técnico de ENTerritorio S.A. en la administración de las soluciones adquiridas durante el plazo de ejecución del contrato.
17. Ante eventuales ataques dirigidos o cualquiera de sus derivados en el ámbito de seguridad que esté contenido dentro de la solución propuesta y que llegue afectar la seguridad en la red de la nube publica de ENTerritorio S.A.S, el contratista durante el plazo de ejecución del contrato deberá proporcionar todo el recurso humano y tecnológico necesario hasta el restablecimiento del servicio en un 100%.
18. Realizar la programación de informes automáticos diarios, semanales y mensuales con los eventos de seguridad de la solución entregada.
19. Entregar la matriz de escalamientos y ANS acordados frente al soporte de la herramienta.
20. Entregar manuales técnicos de uso de la solución ofertada.
21. Brindar asistencia y soporte técnico, por medio telefónico o remoto ilimitado para la solución y atención de requerimientos técnicos, operativos y de información que se puedan presentar.
22. Informar al inicio del contrato los siguientes medios de comunicación y acceso a soporte técnico y actualizaciones:
    - ✓ Número(s) telefónico(s) para soporte.
    - ✓ Dirección de correo electrónico.
    - ✓ Información pertinente y Usuario de contacto para gestión de soporte por diferentes medios, así como el respectivo procedimiento.
23. Realizar todas las actividades que conlleven a la solución de requerimientos técnicos, operativos y de información que se puedan presentar durante la prestación del servicio en un tiempo no mayor a dos días hábiles contados a partir de la recepción de la solicitud.
24. Atender las solicitudes que haga el supervisor del contrato, relacionadas con las dificultades que se puedan presentar, durante la ejecución del objeto contractual en un tiempo no mayor a dos días hábiles contados a partir de la recepción de la solicitud.
25. Las demás que contribuyan a garantizar el cumplimiento del contrato y las que por su naturaleza le sean atribuibles conforme al objeto y alcance de este.

11.3. OBLIGACIONES POR PARTE DE ENTerritorio S.A.

1. Cancelar al CONTRATISTA el valor del contrato en la forma de pago establecida.
2. Exigir al CONTRATISTA la ejecución idónea y oportuna del objeto contractual y velar por el cumplimiento de este.
3. Suministrar la información necesaria que el contratista requiera para la ejecución del contrato.
4. Realizar de manera oportuna los trámites pertinentes por presuntos incumplimientos del contrato.
5. Formular los requerimientos al Contratista para garantizar y propender por la ejecución idónea y oportuna del contrato.
6. Las demás obligaciones que surjan de acuerdo con la naturaleza del contrato.

12. INTERVENTORÍA Y/O SUPERVISIÓN

La supervisión del contrato será ejercida de manera conjunta por el Gerente Grupo de Planeación y Gestión de Riesgos y el Gerente del Grupo de Tecnologías de la Información, así:

El Gerente del Grupo de Gestión de Riesgos: a cargo del uso de la suscripción, solicitudes de soporte técnico, y deberá informar al Gerente del Grupo de Tecnologías de la Información respecto de los requerimientos técnicos relacionados con la suscripción.

El Gerente del Grupo de Tecnologías de la Información (a cargo de los seguimientos de gestión descritos a continuación:

- La gestión que realiza el contratista en el proceso de activación de la suscripción.
- Escalamiento y seguimiento de soporte si ha ello hay lugar.
- La gestión de los procesos de actualización de la suscripción en la infraestructura tecnológica provista.
- El control y seguimiento administrativo, jurídico y financiero del contrato.
- La aprobación de la solicitud de desembolso que el CONTRATISTA le presente, previo cumplimiento de los compromisos establecidos en el contrato y en el presente documento, con el visto bueno de los demás Supervisores.
- La verificación de que el CONTRATISTA se encuentra al día con los pagos a seguridad social y parafiscales, o de las personas que estos designen, quienes de manera permanente realizarán el seguimiento técnico, administrativo, financiero, contable y jurídico del contrato, verificando además la correcta ejecución del objeto contratado.

La supervisión será efectuada de conformidad con lo estipulado en el Manual de Supervisión e Interventoría de ENTerritorio S.A. vigente, por tanto los supervisores realizarán el seguimiento técnico, administrativo, financiero, contable y jurídico del contrato, verificando además la correcta ejecución del objeto contratado.

La designación y notificación de la supervisión la realizará el ordenador del gasto a través del Portal transaccional SECOP II, en el numeral 6 del contrato electrónico “Información presupuestal”, módulo de asignaciones para el seguimiento

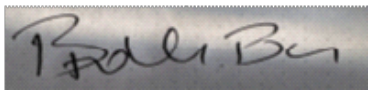
Atentamente,

SANDRA MILLADY RIVEROS BARBOSA
Firmado digitalmente por SANDRA MILLADY RIVEROS BARBOSA

Sandra Millady Riveros Barbosa
Subgerente Administrativa

ARMANDO VIVAS SALAMANCA
Firmado digitalmente por ARMANDO VIVAS SALAMANCA
Fecha: 2024.11.21 09:47:53 -05'00'

Armando Vivas Salamanca
Gerente Grupo de Tecnologías de la Información



Badir Alberto Ali Badran
Gerente Grupo de Gestión de Riesgos

Elaboró: Juan Gabriel Beltrán Dussan – Contratista Grupo Tecnologías de la Información,
Elaboró: Diego Alexander Laverde Duran - Contratista Grupo Tecnologías de la Información,
Elaboró: Jorge Luis Vargas Buitrago – Contratista Grupo de Gestión Riesgos
Revisó: Jhonattan Antonio Acevedo Figueredo - Contratista Grupo Tecnologías de la Información,
Revisó: Carlos Julian Calvete Ferreira – Contratista.

Anexos:
Formato Anexo Análisis De Riesgos F-PR-32
Formato Anexo Esquema De Garantías F-PR-33