DOCUMENTO COMPLEMENTARIO DEL CONTRATO ELECTRÓNICO FNTCE-XXX-2026

Entre los suscritos, **DANIEL AUGUSTO BARRAGÁN SANTOS**, identificado con Cédula de Ciudadanía No. 13.870.909 expedida en Bucaramanga, actuando en calidad Representante **FIDUCOLDEX**, para los asuntos del Patrimonio Autónomo **FONDO NACIONAL DE TURISMO - FONTUR**, con NIT 900.649.119-9, administrado actualmente a través del contrato de Fiducia Mercantil No. 066 de 22 de diciembre de 2023 (número MINCIT 413 de 2023), y, por tanto, comprometiendo única y exclusivamente la responsabilidad del citado Fideicomiso, quien en adelante se denominará **FONTUR** por una parte y por tanto, comprometiendo única y exclusivamente la responsabilidad del citado Fideicomiso, quien en adelante se denominará **FONTUR, ,** por una parte y por la otra, **XXXXXXXXXXXXXXXXXXXXXXXXX** identificada con Cédula de Ciudadanía No. **XXXXXXX** de XXXXX, quien actúa en nombre y representación de la sociedad XXXXXXXXXXXXXX identificada con NIT: XXXXXXXXX, quien en adelante se denominará EL CONTRATISTA, hemos acordado celebrar el Contrato Electrónico No. FNTCE-XXX-2026, el cual se regirá por las normas legales vigentes, y en especial por las siguientes consideraciones y cláusulas:

CONSIDERACIONES

1. Que, la Ley 300 de 1996 creó el Fondo de Promoción Turística cuyos recursos se destinarán a la ejecución de los planes y programas de promoción y mercadeo turístico y a fortalecer y mejorar la competitividad del sector, con el fin de incrementar el turismo receptivo y el turismo doméstico.

2. Que, el artículo 40 de la Ley 1450 de 2011, estableció el Fondo de Promoción Turística, como un instrumento para el manejo de los recursos provenientes de la contribución parafiscal para la promoción del turismo, el cual se ceñirá a los lineamientos de la política turística definidos por el Ministerio de Comercio, Industria y Turismo, siendo preciso establecer que los procesos de contratación que adelante la entidad administradora del Fondo Nacional de Turismo se somete a la legislación privada.

3. El artículo 21 de la Ley 1558 de 2012 dispone que el Fondo de Promoción Turística, que en adelante llevará el nombre de Fondo Nacional de Turismo- P.A. FONTUR, se constituirá como patrimonio autónomo, modificado por la LEY 2294 DE 2023 "POR EL CUAL SE EXPIDE EL PLAN NACIONAL DE DESARROLLO 2022- 2026 "COLOMBIA POTENCIA MUNDIAL DE LA VIDA", **ARTÍCULO 307.** "*Modifíquese el artículo 21 de la Ley 1558 de 2012, el cual quedará así:*

> ***"ARTÍCULO 21.*** *El Fondo Nacional de Turismo -FONTUR- es un patrimonio autónomo, sin personería jurídica, regido por normas de derecho privado, con la función de administrar los recursos señalados en los artículos 1° y 8° de la Ley 1101 de 2006, así como los asignados en el Presupuesto General de la Nación para la infraestructura turística, promoción y la competitividad turística, el recaudo del impuesto al turismo, la contribución parafiscal para la promoción del turismo y las demás fuentes de recursos que señale la ley.*

FONTUR será administrado por la Fiduciaria Colombiana de Comercio Exterior S.A., o la sociedad fiduciaria que determine el Ministerio de Comercio, Industria y Turismo, de acuerdo con los lineamientos que fije éste. La administración y operación del patrimonio autónomo será financiada con cargo a los recursos del FONTUR.

Los recursos del impuesto al turismo, que administra FONTUR, se presupuestarán como una transferencia en el Ministerio de Comercio, Industria y Turismo para cada vigencia".

4. Que, de conformidad con el artículo 307 de la Ley 2294 de 2023, el Patrimonio Autónomo FONTUR será administrado por la Fiduciaria Colombiana de Comercio Exterior S. A., o la sociedad fiduciaria que determine el Ministerio de Comercio, Industria y Turismo, de acuerdo con los lineamientos que fijen este, para este fin se firmó el contrato de Fiducia Mercantil No. 066 del del veintidós (22) de diciembre de 2023 (número MINCIT 413 de 2023).

5. Que, el régimen legal aplicable a los actos y negocios jurídicos de la entidad administradora de FONTUR son exclusivamente las normas del derecho privado. El marco aplicable a la contratación son las normas comerciales y civiles, en cuanto a la calidad del administrador, como encargado de la gestión de los recursos que componen a FONTUR; en consecuencia, se dará rigurosa aplicación a los principios de la contratación del derecho civil, comercial y aquellos señalados en el Manual de Contratación del Patrimonio Autónomo del Fondo Nacional de Turismo – FONTUR.

6. Que, el P.A. FONTUR cuenta con una solución de firewalls implementada, la cual representa una primera línea de defensa ante amenazas de ciberseguridad. Sin embargo, el panorama actual de ciberseguridad ha evolucionado al punto que no basta con proteger únicamente el perímetro, requiere crear más anillos de protección desde la capa de software.

7. Que, aspectos como la adopción del teletrabajo, el uso de dispositivos móviles conectados a la red del FONTUR y la migración de los diferentes aplicativos a la nube de Oracle, aumentan los riesgos de vulnerabilidades de la infraestructura tecnológica, haciendo indispensable la implementación de una estrategia de seguridad integral que contemple protección directa sobre los endpoints y una visibilidad completa de los eventos de seguridad.

8. Que, Para la implementación de una estrategia como la que requiere, es necesario incorporar a la infraestructura tecnológica del patrimonio, los siguientes componentes:

- Una plataforma SIEM para centralizar la gestión de eventos, detectar amenazas en tiempo real y automatizar respuestas. Esta solución permite correlacionar información proveniente de múltiples fuentes (firewall, endpoints, correo, etc.), lo que mejora significativamente la capacidad de detección y respuesta ante incidentes.
- Una solución de protección de endpoints (XDR/EDR) que permitirá detectar y contener amenazas directamente en estaciones de trabajo y servidores, incluyendo ataques sin archivos y amenazas de día cero. Estas soluciones, al integrarse con el SIEM, el sandbox y el firewall existente, garantizan una defensa

coordinada y eficaz en todos los niveles de la infraestructura tecnológica. De igual forma, la protección del correo electrónico y las herramientas colaborativas como Microsoft Teams y OneDrive es crucial para prevenir ataques de phishing, malware y accesos no autorizados.

- Una solución de análisis y gestión de logs, que permite conservar, visualizar y auditar los registros de seguridad de manera estructurada, lo que resulta clave para investigaciones forenses y verificación de políticas.

9. Que, estas soluciones no representan una duplicación de esfuerzos, sino una arquitectura de seguridad en capas que responde a las exigencias actuales del entorno digital. Su implementación permitirá al P.A. FONTUR reducir riesgos de ataques de ciberseguridad, mejorar la capacidad de respuesta ante incidentes, cumplir con normativas vigentes y proteger la continuidad operativa del Patrimonio frente a un panorama de amenazas cada vez más sofisticado. Por lo anterior se requiere la contratación de los siguientes elementos:

Ficha técnica General		
Nro.	**Equipo**	**Cantidad**
1	SIEM - Plataforma correlacionador de eventos	1
2	Protección de correo electrónico y herramientas colaborativas	540
3	LOGS Y REPORTES (ANALIZADOR)	1
4	XDR - Extended Detection and Response	500
5	Servicios Adicionales	1

10. Que, se requiere adelantar la contratación de un proveedor que esté en capacidad de desarrollar las actividades establecidas en las especificaciones técnicas, para lo cual el P.A. FONTUR deberá adelantar un proceso de selección de INVITACIÓN ABIERTA, teniendo en cuenta lo señalado en su Manual de Contratación para llevar a cabo la compraventa para el objeto contractual que se relaciona a continuación: "ADQUIRIR HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR."

11. Que, en sesión del 30 de abril de 2026 se pusieron en consideración de los miembros del Comité de Contratación las condiciones establecidas para el proceso de invitación abierta de que trata esta solicitud de contratación, las cuales fueron aprobadas por el Comité, tal como consta en la certificación expedida por la Secretaría Técnica, en cumplimiento de lo establecido en el Manual de Contratación del P.A. FONTUR, literal i) del numeral 2.6.1. FUNCIONES DEL COMITÉ DE CONTRATACIÓN, según el cual el Comité de Contratación debe "Analizar las condiciones establecidas en los procesos de invitación abierta, invitación cerrada y comparación de cotizaciones, para recomendar o no dar inicio al proceso de selección."

12. Que, dando cumplimiento a lo establecido en el Manual de Contratación en el Numeral 3.1.1. del Capítulo III, la Directora (E) de Estructuración Precontractual del **P.A. FONTUR,** mediante Memorando DEP-85754 de fecha 7 de mayo de 2026, solicitó a la Dirección de Gestión Contractual y Poscontractual de **FONTUR** adelantar la contratación que tiene por objeto: "*CONTRATAR LA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR".*

13. Que, **FONTUR**, adelantó la **Invitación Abierta FNTIA-016-2026** dentro de la cual se presentaron como proponentes:

No.	Proponentes
1.	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
2.	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
3.	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

14. Que, una vez realizada la evaluación de las propuestas recibidas por parte del Grupo Evaluador, fue seleccionada la propuesta presentada por el proponente **XXXXXXXXXXX** quien cumplió con los requisitos habilitantes y obtuvo el mayor puntaje.

15. Que, mediante Documentos de Disponibilidad Presupuestal No. No. 346 del 3 de diciembre de 2025 (recursos fiscales) No. 631 del 3 de diciembre de 2025 (recursos parafiscales) y No. 319 del 20 de marzo de 2026 (recursos parafiscales), expedido por la Unidad de cumplimiento de operaciones financieras del P.A. FONTUR, se certificó la disponibilidad presupuestal para la suscripción del presente Contrato.

16. Que, mediante comunicación de selección publicada en la plataforma Secop II, el día XXX del 2026, se procede a la suscripción del presente contrato.

Efectuadas las anteriores consideraciones, las partes acuerdan las siguientes:

CLÁUSULAS

PRIMERA. OBJETO: "ADQUIRIR HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR".

SEGUNDA. CARACTERÍSTICAS TÉCNICAS ESPECÍFICAS

2.1. FICHA TÉCNICA GENERAL

Ficha técnica General			
Nro.	**Equipo**	**Cantidad**	**Descripción**
1	SIEM - Plataforma correlacionador de eventos	1	Equipo
2	Protección de correo electrónico y herramientas colaborativas	540	Licencias
3	LOGS Y REPORTES (ANALIZADOR)	1	Equipo
4	XDR - Extended Detection and Response	500	Licencias
5	Servicios Adicionales	1	Soporte y Mantenimiento

2.2. SIEM - PLATAFORMA CORRELACIONADOR DE EVENTOS

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
La solución SIEM deberá permitir el monitoreo y correlación de eventos de seguridad de la información

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
provenientes de los diferentes dispositivos a correlacionar. Se deberán definir los casos de uso en conjunto con el patrimonio al momento de la implementación del servicio.
Generalidades: • Analítica de red en tiempo real • Seguridad y conformidad listas para usar • Un único panel de Administración • Arquitectura a escala de la nube • Autoaprendizaje del Inventario de activos (CMDB) • Multitenant • Correlación cruzada de analítica de SOC y NOC • Asignaciones de reglas de TI e ICS de MITRE ATT&CK y visibilidad de la cobertura • La solución debe ser una plataforma de hardware de propósito especifico que se entregue completamente licenciada y con soporte. Adicionalmente de estar en capacidad de escalar en cuanto a capacidades de Eventos por Segundo y Dispositivos.
Se deben documentar todos los casos de uso implementados y estos deben hacer parte de la entrega del servicio una vez finalice.
Solamente se deben tener fuentes de información integradas, que tengan reglas asociadas, evitando que se pueda tener una ingesta sin valor.
La solución deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por el P.A FONTUR, como mínimo deberán observarse las resoluciones, directrices y lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINTIC y los controles del anexo A de la norma técnica ISO 27001:2022.
La solución debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información y mantener el inventario actualizado de dispositivos monitoreados de la solución SIEM.
La solución debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo con los niveles de servicio.
Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad del Patrimonio y podrán ser solicitadas en cualquier momento para atención de requerimientos legales. El servicio debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo con los niveles de servicio.
Se deben generar alertas de otras amenazas que puedan impactar la infraestructura del Patrimonio, como las identificadas en los reportes de análisis de tendencia de centros SIRT/CERT o en las bases de datos de conocimiento del contratista.
El servicio de monitoreo SOC deberá mantener sincronizados todos los relojes de la herramienta SIEM con la hora legal colombiana, suministrada por el Instituto Nacional de Metrología de Colombia (https://inm.gov.co/web/servicios/hora-legal/).
La herramienta deberá garantizar la optimización en la ingesta y procesamiento de eventos con los siguientes criterios: • Evitar la integración de fuentes sin uso real, asegurando que todos los eventos ingeridos sean relevantes y aporten valor a la detección de amenazas. • Garantizar la integración de fuentes críticas, priorizando NGFW, DDI, autenticación y acceso en servidores Microsoft, servidores no Microsoft (no centralizado) y plataformas colaborativas/correo. • Brindar visibilidad sobre servidores con autenticación local, permitiendo el monitoreo y correlación de accesos en entornos que no dependen de un directorio centralizado. • Monitorear aplicaciones con autenticación local, asegurando que los accesos sean controlados y correlacionados con otras fuentes de seguridad. • Incluir la ingesta de eventos de plataformas colaborativas y correo, asegurando visibilidad y detección de amenazas en estos entornos clave.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
• Aplicar inteligencia artificial y machine learning (IA/ML) para la detección de anomalías y amenazas avanzadas, reduciendo la dependencia de reglas estáticas y minimizando falsos positivos. • Optimizar la relación costo-beneficio de la ingesta en el SIEM, asegurando que los eventos procesados sean los más relevantes para la seguridad del patrimonio.
La solución debe estar actualizada y permitir recopilar, almacenar y correlacionar datos de registros además de contar con capacidad de generar informes de cumplimiento. • Recopilación y correlación de registros • Gestión de registros • Generador de informes y paneles gráficos
Debe contar con la capacidad de almacenar logs de seguridad para propósitos forenses e investigación y los correspondientes eventos por el periodo definido por el P.A. FONTUR.
Debe contar con actualizaciones de firmas, amenazas, URLs y demás funcionalidades de seguridad ante las cuales pueda proteger el(os) dispositivo(s) que hagan parte de la solución SIEM instalada y actualizaciones de fabricante durante la duración del servicio.
Debe contar con suministro, instalación, actualización y configuración de las licencias y actualizaciones de todos los productos que compongan la solución SIEM en su totalidad e integridad, durante todo el tiempo del contrato.
Debe ser alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso.
Debe de poseer una arquitectura de carga equilibrada incorporada para recopilar eventos de sitios remotos a través de coleccionistas.
Debe permitir administrar múltiples grupos de dispositivos y usuarios (grupos) con una sola implementación. Dispositivos y direcciones IP pueden traslaparse entre grupos organizacionales.
Debe proveer estricta separación lógica entre grupos organizacionales en la capa de aplicación.
Debe poder recopilar una amplia variedad de métricas de rendimiento y disponibilidad. También debe alertar cuando las métricas están fuera de un perfil definido y correlacionar tales violaciones con problemas de seguridad.
Debe proporcionar mecanismos para rastrear y detectar cambios de archivos clave. Debe monitorear la configuración de inicio y ejecución de dispositivos de red a través de SSH. Debe monitorear archivos de configuración en servidores. Debe monitorear infraestructuras de servidores. Debe alertar cuando un archivo cambia de una versión a otra.
Debe verificar la identidad de usuario y seguimiento de ubicación; al combinar registros de DHCP, registros de VPN, registros de WLAN, eventos de inicio de sesión del controlador de dominio, debe mantener un seguimiento de auditoría para la dirección IP para el usuario y las asignaciones de ubicación geográfica a lo largo del tiempo.
La solución debe tener un marco flexible para conectarse a una amplia variedad de fuentes de amenazas (tanto gratuitas como de pago), descargar esta información y encontrar coincidencias en tiempo real en el entorno en el que se está ejecutando, integrando inteligencia de amenazas externas.
Debe permitir la puntuación y riesgo de usuario y dispositivo; al combinar la criticidad de los activos, el rol y la criticidad del usuario, la gravedad del incidente, la frecuencia de ocurrencia y las vulnerabilidades encontradas. Debe asignar una calificación de riesgo a los usuarios y las máquinas. Este puntaje se debe mostrar en un tablero con capacidades de desglose para identificar los factores subyacentes.
Debe proporcionar informes haciendo uso de plantillas de búsqueda, según el tipo de dispositivo y la funcionalidad, como disponibilidad, rendimiento, cambio y seguridad. Capacidad de unificación de eventos y las capacidades de profundización o búsqueda de amenazas.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
Debe proporcionar paneles para visualización de los datos que se recopilan y los incidentes de seguridad que se han detectado.
Debe poseer un sistema de tickets incorporado para administrar incidentes a través de tickets. Admitir el ciclo de vida completo de apertura, escalado, cierre, reapertura y creación de casos con archivos adjuntos para evidencia.
Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls.
Estado del sistema a través de SNMP, WMI, PowerShell.
Estado de aplicaciones a través de JMX, WMI, PowerShell.
Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.
Uso de almacenamiento, monitorización de rendimiento - EMC, NetApp, Nutanix, Nimble, DELL, HP.
Monitorización del rendimiento de aplicaciones a medida.
Microsoft Active Directory y Exchange a través de WMI y Powershell.
Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.
Infraestructura VoIP a través de IPSLA, SNMP, CDR / CMR.
Análisis de flujo y rendimiento de la aplicación – Netflow v5 y v9, SFlow, JFlow, Cisco AVC e IPFIX.
Posibilidad de agregar métricas personalizadas.
Métricas de base y detección de desviaciones.
Notificación y Gestión de Incidentes • Framework de notificación de incidentes basado en políticas. • Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. • Integración basada en API a sistemas externos de ticketing - ServiceNow, Salesforce, ConnectWise, Remedy y Jira. • Sistema incorporado de ticketing.
Paneles de control personalizados • Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs. • Informes y análisis exportables entre organizaciones y usuarios. • Identificación rápida los problemas críticos, por ejemplo, a través de un código de colores. • Actualización rápida mediante el cálculo en memoria, sin acceso a disco. • Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas.
Integración con fuentes de Inteligencia Externas • API para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor, etc. • Integración para fuentes de inteligencia de amenazas populares - ThreatStream, CyberArk, SANS, Zeus, etc. • Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real.
Analítica • Búsqueda de eventos en real - sin necesidad de indexación. • Búsquedas por palabras clave basadas en atributos de eventos analizados. • Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
• Match de patrones complejos en tiempo real. • Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. • Programación de informes y entregas de resultados por correo electrónico a los principales interesados. • Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). • Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. • Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. • Análisis escalable mediante la adición de nodos worker en caliente. • Posibilidad de priorización de los informes de incidentes.
Licenciamiento • El fabricante ofertante deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados, pudiendo elegir al menos entre licencias perpetuas y modo suscripción. • Se deberá disponer de paquetes de licencia de agentes avanzados para monitorización de servidores críticos Windows y Linux, tanto en modo perpetuo como modo suscripción. • Se deberá disponer de otras suscripciones como Indicadores de Compromiso (IoC). • Se deberá poder añadir EPS adicionales sin necesidad de contratar soporte asociado a los mismos. • Se podrán desplegar tantos colectores virtuales como se quiera sin coste adicional.
Dimensionamiento: • Numero de Eventos por Segundo (EPS): 1000 • Numero de dispositivos soportados/licenciados: 100 • Número de agentes para Logs y FIM (File Integrity Monitoring): 50 • Número de puntos de IoC: 200 El Patrimonio requiere que la plataforma SIEM sea un appliance de propósito especifico con las siguientes características de desempeño basado en las variables de dimensionamiento: • CPU: 2 x Intel Xeon Silver 4210R 10C20T 2.4GHz • Memoria: DDR4 128GB • Capacidad de Almacenamiento: 4TB HDDs (32TB) y 1.92TB SSDs • Capacidad Maxima (EPS): 20K EPS • Maximo Número de Usuarios UEBA: 10.000

2.3. SERVICIO PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS COLABORATIVAS

Especificaciones técnicas - Protección del Entorno de Trabajo
Generalidades • La solución debe actualizarse automáticamente • La solución debe proveer la seguridad del sitio de trabajo a través de protección del correo electrónico, browsers y plataformas de colaboración, que incluya protección contra phishing, ransomware, ataques de día cero y apropiaciones de cuentas en una sola consola para 540 usuarios. • La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales • La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales • La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para

Especificaciones técnicas - Protección del Entorno de Trabajo
una protección completa en M365 como mínimo • La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico • La solución debe ser implementada automáticamente con la integración de Office 365 y Google Mail • La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones • La solución debe integrarse con Office 365 a través de API sin necesidad de cambiar el registro MX • La solución debe poderse ajustar a las políticas y SIEM existentes y no requiere cambios en la infraestructura e integración vía REST APIs • La solución debe estar en capacidad de exportar registros en tiempo real al SIEM del Patrimonio • La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML • Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC • La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador • La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+ • Las claves de cifrado deben estar protegidas con soluciones como AWS KMS • La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001 • La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio • La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas • La solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc. • La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación • El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugués • La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto • La solución debe enviar informes y resúmenes de acciones a los usuarios
Protección de Correo Electrónico • La solución debe analizar dinámicamente el 100% de los correos electrónicos • La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes • La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos • El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso • La solución debe proteger activamente contra el spam • La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente • La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas • La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos • La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus • La solución debe utilizar herramientas para identificar firmas muy complejas • La solución debe proteger contra los ataques de phishing a través del reconocimiento de

Especificaciones técnicas - Protección del Entorno de Trabajo
imágenes, el análisis de texto y los evaluadores de reputación • La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC • La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP • La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU • La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario • La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final • La solución contar con la tecnología Sandbox para identificar archivos maliciosos • La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos • La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos • La solución debe identificar vulnerabilidades de daño en la memoria • La solución debe detectar errores lógicos y macros dentro de los documentos • La solución debe escanear cientos de tipos de archivos diferentes • La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear • La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad • La solución debe analizar contenido protegido con contraseña al entregarse la contraseña • La solución debe analizar archivos comprimidos/comprimidos • La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico • La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.
Navegación Segura (Protección de Navegadores) • La solución debe bloquear sitios de phishing de hora cero, sitios maliciosos, extensiones peligrosas en el browser en tiempo real. • La solución debe instalar un agente liviano que no afecte el funcionamiento del navegador • La solución debe proveer una consola donde se indique un inventario de usuarios y browsers utilizados • Debe permitir el modo de protección de riesgos (Silencioso, precaución, Bloqueo como mínimo) • Debe permitir personalizar las interfaces de usuario final para enviar precauciones, mensajes o bloqueos • Debe permitir la integración con SAML • Debe permitir asignar políticas con base en los permisos del usuario (atributos de SAML) • Debe permitir el uso de Roles (RBAC) • Debe permitir crear usuarios de administración y auditoria • Debe estar en capacidad de realizar una correlación entre eventos del Browser y el correo. • Debe soportar sistemas operativos Windows, MacOS, Chrome OS, LinuxOS. • Debe cumplir la integración con soluciones UEM para la implementación como Microsoft Intune, Jumpcloud, Jamf Pro, Google Workspace. • La solución debe usar modelos de Inteligencia Artificial para reconocimiento de imágenes y texto • La solución debe permitir la instalación por medio de invitación de correo • Debe ser compatible con cualquier infraestructura de red/proxy/VPN. • La solución debe reforzar el acceso seguro a las aplicaciones web y SaaS mediante DLP para prevenir fuja de datos accidental o intencional interna o externa. • La solución debe estar en capacidad de detener descargas de archivos y exploits de secuencias de comandos entre sitios (XSS)

Especificaciones técnicas - Protección del Entorno de Trabajo
• La solución debe estar en capacidad de administrar Google Chrome, Microsoft Edge, Firefox, Safari y cualquier otro browser con base en Chromium (ej Opera, brave, Arc, etc.)
Protección de Herramientas de Colaboración • La solución debe ser compatible con Slack, Microsoft 365 (Teams, OneDrive, SharePoint), Google Drive, Box, Salesforce, Dropbox, Zendesk, AWS S3 Buckets y otras aplicaciones usando APIs. • La solución debe detectar y bloquear archivos maliciosos, URLs, y ataques avanzados en las soluciones protegidas • Debe escanear el 100% de los datos • La solución debe evaluar los correos y URLs que se envíen por las plataformas evaluadas • El servicio debe tener un Objetivo de nivel de servicio de mínimo 99.98% • Debe proveer servicios de Análisis de amenazas, Análisis dinámico y estático de archivos, protección de toma de cuenta (mínimo MS365) • Debe proveer Gobernanza de los navegadores y DLP
Servicio • La solución debe contar con un equipo interno de Incident&Response (IR) para reforzar los servicios de detección y corrección de los correos • La solución debe proporcionar servicios complementarios de equipos Incident&Response (IR) como parte de la oferta sin cargo adicional • La solución debe ofrecer soporte al cliente y capacitación ilimitados según sea necesario sin cargo adicional durante la duración del contrato • El servicio de atención al cliente debe estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.

2.4. SERVICIO DE LOGS Y REPORTES (ANALIZADOR)

Especificaciones Técnicas - Logs y reportes
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interfaz gráfica (GUI) como vía línea de comandos en consola de gestión.
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
Soporte SNMP versión 2 y 3
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
Debe permitir activar y desactivar para cada interfaz de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
Autenticación de usuarios de acceso a la plataforma vía LDAP Autenticación de usuarios de acceso a la plataforma vía Radius Autenticación de usuarios de acceso a la plataforma vía TACACS+
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja. Generación de informes en tiempo real de tráfico, en formato de gráfica tabla

Especificaciones Técnicas - Logs y reportes
Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña de este.
Permitir la importación y exportación de reportes • Debe contar con la capacidad de crear informes en formato HTML • Debe contar con la capacidad de crear informes en formato PDF • Debe contar con la capacidad de crear informes en formato XML • Debe contar con la capacidad de crear informes en formato CSV • Debe permitir exportar los logs en formato CSV
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora de este.
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
Debe ser posible la duplicación de reportes existentes para su posterior edición.
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.
Debe permitir descargar de la plataforma los archivos de logs para uso externo.
Tener la capacidad de generar y enviar reportes periódicos automáticamente.
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
Permitir el envío por email de manera automática de reportes.
Debe permitir que el reporte a enviar por email sea al destinatario específico.
Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
Debe permitir visualizar en tiempo real los logs recibidos.
Debe permitir el reenvío de logs en formato syslog.
Debe permitir el reenvío de logs en formato CEF (Common Event Format).

Especificaciones Técnicas - Logs y reportes
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en su red.
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
Debe permitir crear dashboard personalizados para monitoreo de operaciones SOC
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
Debe permitir generar alertas de eventos a partir de logs recibidos
Debe permitir crear incidentes a partir de alertas de eventos para endpoint
Debe permitir la integración al sistema de tickets ServiceNow
Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
Debe permitir respaldar logs en nube publica de Amazon S3
Debe permitir respaldar logs en nube publica de Microsoft Azure
Debe permitir respaldar logs en nube publica de Gooogle Cloud
Debe soportar el estándar SAML para autenticación de usuarios administradores
Los siguientes hacen referencia a los Reportes asociados a la actual Arquitectura Fortinet del Patrimonio. Reportes para Fortigate: • Debe contar con reporte de cumplimiento de PCI DSS • Debe contar con reporte de utilización de aplicaciones SaaS • Debe contar con reporte de prevención de perdida de datos (DLP) • Debe contar con reporte de VPN • Debe contar con reporte de Sistema de prevención de intrusos (IPS) • Debe contar con reporte de reputación de cliente • Debe contar con reporte de análisis de seguridad de usuario • Debe contar con reporte de análisis de amenaza cibernética • Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad • Debe contar con reporte de tráfico DNS • Debe contar con reporte tráfico de correo electrónico • Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red • Debe contar con reporte de Top 10 de Websites utilizadas en la red • Debe contar con reporte de uso de redes sociales
Reportes Soluciones de Protección de Correo:

Especificaciones Técnicas - Logs y reportes
• Debe contar con reporte de evaluación de riesgo para correo electrónico Reportes solución Wireless: • Debe contar con reporte de cumplimiento PCI de Wireless. • Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WiFi Reportes WAF • Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web
El proveedor entregará un equipo de propósito especifico. La solución de análisis de logs debe dar soporte a las siguientes características: • Capacidad de recibir hasta 25 GB de logs diarios. • Capacidad de Almacenamiento de 4 Terabytes • 2 interfaces de red de 1Gbps Mbps Cobre • Capacidad de recibir logs hasta de 50 equipos sin necesidad de licencias adicionales

2.5. XDR - EXTENDED DETECTION AND RESPONSE

Especificaciones Técnicas - XDR - Extended Detection and Response
Generalidades • El Patrimonio requiere del licenciamiento de la solución xDR/EDR para 500 dispositivos. • La solución de xDR/EDR debe proporcionar al Patrimonio un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas.
Funcionalidades de Prevención: • El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional. • Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML) • Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube que se actualiza continuamente. • Proteger los endpoints desconectados de la red con una protección fuera de línea; este modo de operación se denomina modo autónomo. • Proporcionar un control de dispositivos USB basado en múltiples parámetros. • Debe estar en capacidad de eliminar tiempos de permanencia y Fatigas por exceso de alamas (falsos positivos) • Gestión de parches para sistemas operativos Windows, OS, Linux.
Funcionalidades de Descubrimiento: • El xDR/EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad • Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT. • Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad. • Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior • Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables • Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.
Funcionalidades de Detección y Protección:

Especificaciones Técnicas - XDR - Extended Detection and Response
• El xDR/EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad del Patrimonio. Tan pronto como el xDR/EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado, debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del xDR/EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes items: ○ Se debe basar en la detección integrada de forma profunda en el sistema operativo, permitiendo la detección de ataques de infiltración sigilosa, los ataques basados en la memoria y los ataques "living off the land". ○ Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows). ○ Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa. ○ Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control. ○ Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros. ○ Debe Permitir definir listas blancas y negras para personalizar mediante exclusiones estas protecciones (por hash, nombre y/o ruta de archivo, o por aplicación, incluyendo datos de versión y fabricante). ○ Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares. ○ Debe Proporcionar un análisis de todo el historial de eventos. ○ Debe realizar la validación continua de la clasificación de amenazas.
Funcionalidades de Protección contra Ransomware: La solución de xDR/EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo: • Debug de Procesos. • Código dinámico. • Formato de archivo ejecutable incorrecto • Una pila con código ejecutable • El programa ejecutado no tiene instalador • Programa crítico falso. • Empaquetador falso. • File Encryptor. • Proceso oculto. • Ejecutable inyectado. • Proceso inyectado. • Hilo inyectado. • Suma de comprobación no válida. • Ejecución no válida. • Puntero no válido.

Especificaciones Técnicas - XDR - Extended Detection and Response
• Inyección de kernel. • Empaquetador conocido. • Archivo malicioso detectado. • Proceso malicioso. • Ejecutable modificado. • Stack Parcialmente asignado. • Exploit de escalamiento de privilegios. • Proceso vacío. • Manipulación de pilas. • Aplicación sospechosa. • Empaquetador sospechoso. • Ejecutable manipulado. • Ejecutable no confirmado. • Ejecutable sin asignar. • Código grabable. • Prevención automatizada en tiempo real cifrado de Ransomware
Funcionalidades de Remediación: • La Solución de xDR/EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno del Patrimonio, las características de remediación deben cumplir como mínimo con los siguientes requerimientos: • Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta. • Debe estandarizar los procedimientos de respuesta a incidentes con la automatización de playbooks • Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la apertura de tickets. • Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como, por ejemplo, grupos de estaciones de trabajo). • Debe proporcionar visibilidad completa de la cadena de ataque y los cambios maliciosos, mediante el seguimiento de código. • Debe permitir automatizar la limpieza y reversión de los cambios maliciosos preservando así la integridad del sistema. • Debe realizar la contención y respuesta de forma automática • Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
Funcionalidades de Investigación: • La solución de xDR/EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoints infiltrados. La interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos: • Debe desactivar y bloquear automáticamente las amenazas, lo que permite a los analistas de seguridad cazar marcando sus propios tiempos. • Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el "paciente cero", incluso si el dispositivo está fuera de línea. • Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.

Especificaciones Técnicas - XDR - Extended Detection and Response
• La interfaz gráfica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.
Funcionalidades de xDR/EDR: La solución de xDR/EDR debe tener la capacidad de poder integrarse con diferentes plataformas de seguridad, creando así un marco robusto que pueda identificar y responder eficiente y eficazmente frente a los ataques como es recomendado por Gartner. La solución de xDR/EDR debe poder integrarse con las siguientes plataformas: • Next Generation Firewall del Patrimonio. • Control de Acceso a la Red (NAC). • Sandboxing del presente proceso. • Deception o HoneyPots • Correlacionador de Eventos, SIEM del presente proceso. • Plataformas de Orquestación, automatización y respuesta a incidentes, SOAR. • Plataformas de Análisis de comportamiento de usuario UEBA • Plataformas de Manejo de Identidades, IAM
Componentes de la Solucion xDR/EDR: • Debe contar con una Gestión Unificada. • Debe contar con la funcionalidad de IDENTIFICACIÓN DE INCIDENTES ENTRE PRODUCTOS • Debe contar con la funcionalidad de INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL • Debe contar con la funcionalidad de RESPUESTA AUTOMATIZADA • La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de una agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos, en versiones de 32 y 64 bits: • Windows: XP SP2/SP3, 7, 8, 8.1 y 10. • Windows Server: 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 y 2019. • MacOS: Yosemithe (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15). • Linux: Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, y Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, en 64-bit. • Entornos VDI: VMWare Horizons 6 y 7, y Citrix Desktop 7. • En cuanto al hardware, se debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco. • Adicional la solución debe permitir ser desplegada de cualquiera de las siguientes maneras: • Nube: En la Nube del Fabricante. • On-Premise: En el Datacenter del Patrimonio. • Hibrida: En Nube y On-premise. • AirGapped o Sistemas Cerrados.

2.6. SERVICIOS ADICIONALES

Soporte y Garantía	El contratista deberá brindar soporte con atención de 24x7x365 que permita atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas en horario hábil y no hábil, con cambio de partes por un (1) año. El proponente deberá registrar, documentar, atender y resolver los casos reportados, permitiendo garantizar el correcto funcionamiento de todas las soluciones ofertadas. Las diferentes tareas estarán enmarcadas en: • Resolución de problemáticas asociadas al funcionamiento de las soluciones.

<table>
<tr>
<td></td>
<td>

Gestionar con los especialistas del P.A. FONTUR los diferentes casos que se presenten con el objetivo de dar solución a las problemáticas y /o incidencias de las soluciones.

El servicio de soporte técnico deberá permitir el escalamiento (hacia las diferentes áreas funcionales del P.A. FONTUR) de las diferentes problemáticas y/o incidencias, documentando los errores presentes o futuros a nivel del servicio. Así mismo el servicio de soporte técnico deberá permitir los respectivos escalamientos en caso de que las plataformas que soportan el servicio entren en fallo o requieran configuraciones especiales para garantizar el correcto funcionamiento.
El contratista podrá brindar el soporte inicial de manera remota con el fin que se ofrezca una respuesta rápida y efectiva, minimizando los tiempos de respuesta y optimizando la resolución de cualquier incidencia que pueda surgir.
El oferente deberá garantizar los siguientes ANS que se detallan en los tiempos de atención de seguridad u operación, este tiempo se define como el transcurrido entre el registro del incidente y el inicio de la atención de este por parte de un especialista de soporte y servicio técnico.
<table>
<tr><th rowspan="2">INCIDENTE</th><th rowspan="2">TIEMPO DE NOTIFICACIÓN</th><th colspan="2">TIEMPOS DE RESPUESTA</th></tr>
<tr><th>Nivel 1</th><th>Nivel 2</th></tr>
<tr><td>Crítico</td><td>15 min.</td><td>30 min.</td><td>1 hora</td></tr>
<tr><td>Alto</td><td>30 min.</td><td>1 hora</td><td>1 hora</td></tr>
<tr><td>Medio</td><td>4 horas</td><td>6 horas</td><td>12 horas</td></tr>
<tr><td>Bajo</td><td>8 horas</td><td>12 horas</td><td>24 horas</td></tr>
</table>
Prioridad Crítica: Situación que se presenta y genera pérdida total del servicio en el ambiente de producción por indisponibilidad de todas las componentes críticas del mismo. La afectación genera un impacto catastrófico para el negocio.
Prioridad Alta: Situación que se presenta y genera impacto mayor para el negocio sobre el servicio por indisponibilidad de algunos componentes críticos del mismo.
Prioridad Media: Situación que se presenta y genera un impacto moderado para el negocio por degradación de algunos componentes del servicio.
Prioridad Baja: Situación que se presenta pero que no genera afectación del servicio. Se trata de un evento que no impide en forma alguna la operación y el impacto para el negocio es menor.
Nota: Los servicios de soporte en sitio se acordarán con el personal técnico y especialistas del P.A. FONTUR.
</td>
</tr>
<tr>
<td>Servicios Profesionales</td>
<td>
Se debe realizar la instalación, configuración, actualización y puesta en marcha de las soluciones ofertadas.
El contratista deberá realizar y ejecutar un protocolo de pruebas para la entrega a satisfacción de la solución, el cual será aprobado por el Supervisor del contrato.
Se deben realizar las respectivas pruebas de funcionalidad y operatividad de todos y cada uno de los elementos, con el propósito de comprobar la calidad y cumplimiento de los requerimientos solicitados.
</td>
</tr>
</table>

	Presentar plan de trabajo y cronograma de trabajo dentro de los cinco (5) días siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar. La implementación deberá comprender los siguientes puntos: • Diseño y planeación de cada una de las actividades minimizando la afectación del servicio. • Instalación de equipos • Configuración y alistamiento de la plataforma a la última versión estable aprobada por el fabricante. • Implementación de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura. • Pruebas de Servicio. • Puesta en Producción. • Estabilización de la plataforma. • Plan de mantenimientos preventivos.
Transferencia de Conocimiento	El Contratista debe realizar transferencia de conocimiento técnico para los especialistas que el P.A. FONTUR designe con una intensidad horaria de veinte (20) horas, sobre la operación y administración de las soluciones objeto del presente proceso contractual. Los servicios de transferencia de conocimiento de las soluciones objeto del presente proceso contractual, están definidos en el presente documento de oferta. El oferente seleccionado deberá realizar una transferencia de conocimiento funcional de las soluciones desplegadas, donde se informará a los integrantes del personal técnico del P.A. FONTUR sobre la arquitectura y las funcionalidades de las soluciones y herramientas desplegadas, además, se dará instrucción sobre la administración básica de la plataforma y el despliegue de los casos de uso de las funcionalidades configuradas. **Nota:** En ningún caso esta transferencia de conocimiento equivaldrá a un curso oficial del fabricante, debido a que estos cursos oficiales son impartidos únicamente por Learning Partners oficiales del fabricante.
Documentación	Plan de implementación que indique tiempos, actividades, posibles afectaciones, riesgos y mitigación de estos, previo al inicio de la instalación. Informe de diagnóstico y recomendaciones sobre la plataforma de Seguridad del Patrimonio, basado en mejores prácticas. Documento técnico de implementación de las soluciones contratadas, haciendo énfasis en las configuraciones realizadas.
Certificados	1. **Certificación Distribuidor Autorizado:** El proponente deberá aportar y contar con certificación como distribuidor autorizado para hacer suministro, instalación y configuración de los equipos de la marca a ofertar para las soluciones y herramientas relacionadas en el anexo técnico, con el máximo nivel de la membresía en Colombia. Dicha certificación deberá ser expedida por el fabricante y/o el distribuidor oficial de la marca para Colombia, la cual deberá estar dirigida al P.A. FONTUR, con fecha no mayor a 30 días de expedida al cierre de la presentación de las ofertas. 2. **Certificación de Especialidades:** El oferente deberá allegar certificación expedida por el fabricante, para los elementos relacionados en el anexo técnico

	donde acreditará que cuenta con mínimo cinco (5) de las siguientes especialidades: a. Operational Technology b. Public Cloud Security c. SD-WAN d. Security Operations e. SASE f. Secure Networking LAN g. Secure Networking Firewall h. Zero Trust Network Access (ZTNA) 3. El proponente deberá aportar certificación ISO 22301 gestión de continuidad del negocio. 4. El oferente debe contar con su propio SOC, deberá presentar junto con su propuesta, el certificado ISO 27001 DEL 2022 (SGSI) para su proceso de SOC y la certificación de membresía de First. **Nota:** El proponente deberá ofrecer dentro de su propuesta productos de primera calidad, libres de defectos e imperfecciones y de Marcas reconocidas a nivel mundial en el mercado del sector de las TIC, lo cual deberá realizar en el formato establecido por el P.A. FONTUR y en el que se indicará lo siguiente: Marcas, modelos y referencias de los bienes ofertados. Por lo que no se aceptarán marcas genéricas, equipos que sean clones, remanufacturados o reconstruidos, para de esta manera mitigar riesgos en los servicios posventa y garantizar la calidad de los equipos tecnológicos adquiridos. Además, deberán cumplir los estándares de calidad exigidos en el mercado, de conformidad con las especificaciones técnicas establecidas y exigidas por el Patrimonio.

2.7. PERSONAL MÍNIMO REQUERIDO

ROL	PERFIL	EXPERIENCIA	CERTIFICACIONES
Gerente de Proyecto	Profesional en Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de Sistemas y/o afines según área de conocimiento clasificación SNIES. Con postgrado en Sistemas Gerenciales de Ingeniería o Gerencia de	**Experiencia General:** Siete (7) años de experiencia a partir de la expedición de la tarjeta profesional. **Experiencia Específica:** Cinco (5) años de experiencia como líder de implementación en conocimiento	Contar con al menos tres (3) certificaciones vigentes de las siguientes: • PMP • SFPC (Scrum Foundation Professional Certificate). • Auditor Líder 27001:2013/2022. • Cisa (Certified Information Systems Auditor). • CISM (Certified Information Security Manager).

	Proyectos o Especialista en Seguridad de la Información. Deberá contar con Matrícula Profesional vigente y Certificado de antecedentes disciplinarios emitidos por el Consejo Profesional Nacional de Ingeniería – COPNIA.	y gestión de proyectos.	
Líder de Instalación y Conectividad	Profesional en Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de sistemas y/o afines según área de conocimiento clasificación SNIES.	**Experiencia General:** Cuatro (4) años de experiencia a partir de la expedición de la tarjeta profesional. **Experiencia Específica:** Cuatro (4) años de experiencia como líder de implementación en conocimiento y gestión de proyectos.	El Ingeniero líder de instalación y conectividad deberá presentar al menos tres (3) de las siguientes certificaciones: • Fortinet Certified Professional Secure Networking. • Fortinet Certified Professional Security Operations. • Fortinet Certified Solution Specialist Secure Networking. • Fortinet Certified Solution Specialist Security Operations. Las certificaciones deberán corresponder a las indicadas por el fabricante en los siguientes portales: https://www.fortinet.com/lat/trainingcertification https://www.fortinet.com/lat/corporate/about-us/newsroom/pressreleases/2023/fortinet-expands-nsecertification-program-to-addressevolving-cybersecurity-skillset-needs
Líder de Ingeniería - Implementador	Profesional en Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de sistemas	**Experiencia General:** Diez (10) años de experiencia a partir de la expedición de la tarjeta profesional.	Contar mínimo con cinco (5) certificaciones vigentes de las siguientes especialidades: • Cisa (Certified Information Systems Auditor). • CISM (Certified Information • Security Manager). • Itil 4 (Itil Foundation Certificate in IT Service

	y/o afines según área de conocimiento clasificación SNIES. Posgrado en: Seguridad de las tecnologías de la información y/o de las comunicaciones o administración de riesgos informáticos y/o seguridad informática.	**Experiencia Específica:** Siete (7) años de experiencia como líder de implementación en conocimiento y gestión de proyectos.	• Management). • ISO 27032:2012 (Lead Cybersecurity Manager). • ISO 27001:2013 (Auditor Líder). • ISO 22301: 2012 (Sistema de Gestión de Continuidad • del Negocio). • SFPC (Scrum Foundation Professional Certificate). • CEH (Certified Ethical Hacker). Conocimiento técnico en configuración de políticas de filtrado de contenido, inspección de tráfico de correo, cifrado, cuarentena y protección frente a amenazas avanzadas.

PARÁGRAFO PRIMERO: La verificación de las hojas de vida de los profesionales propuestos para conformar el equipo mínimo requerido será realizada por el supervisor del contrato, una vez iniciada la ejecución contractual. Esta verificación incluirá la validación del cumplimiento de los requisitos de formación académica, experiencia y demás condiciones exigidas en las especificaciones técnicas del presente documento. En caso de encontrarse inconsistencias o incumplimientos, el contratista deberá realizar los ajustes necesarios, incluyendo la sustitución del personal, sin que ello implique costos adicionales para la entidad contratante ni afecte el cumplimiento de las obligaciones contractuales.

Lo anterior sin perjuicio del compromiso de contratación del personal mínimo requerido que deba suscribir el proponente durante el proceso de selección correspondiente.

PARÁGRAFO SEGUNDO: La documentación de hoja de vida y soportes correspondientes al perfil del personal mínimo requerido no será aportada con la oferta; deberán ser presentados por el contratista a la supervisión **dentro de los tres (3) días hábiles a la suscripción del contrato,** para su revisión, verificación y aprobación, previo a la realización de la reunión de inicio del contrato.

El Supervisor realizará la verificación de estos perfiles dentro de los dos (2) días hábiles siguientes a la radicación de estos perfiles por parte del contratista, considerando los requisitos establecidos para cada perfil solicitado; en caso de no presentar el título solicitado en el perfil académico que hace parte del equipo mínimo de trabajo, el Supervisor designado realizará la verificación del título profesional aportado por el proponente en el Sistema Nacional de Información de la Educación Superior SNIES, el cual deberá tener coincidencia en alguno de los campos (Área de conocimiento y/o Núcleo Básico del Conocimiento – NBC) frente alguno de los títulos solicitados por el P.A. FONTUR en el perfil académico. Para la definición de la validez de los títulos aportados, el supervisor verificará la pertinencia de acuerdo con el objeto de la invitación, las actividades a desarrollar y el perfil a desempeñar. En caso de no cumplir con el perfil requerido en la contratación, se otorgará un término adicional de dos (2) días hábiles para que el contratista realice el cambio del profesional a que haya lugar, el cual será objeto de validación por parte

de la supervisión dentro de los dos (2) días hábiles siguientes, en caso de no cumplir con el perfil, se dará aplicación al proceso de incumplimiento que para tal efecto dispone el contrato suscrito entre el P.A. FONTUR y el contratista.

PARÁGRAFO TERCERO: La Experiencia general será contada a partir de la expedición de la Tarjeta Profesional, conforme acreditaciones contractuales o certificaciones emitidas por la entidad donde prestó los servicios, en la cual deberá indicar como mínimo: Datos de la entidad pública y/o privada, fecha de inicio y fecha de terminación y cargo o profesión.

PARÁGRAFO CUARTO: La Experiencia específica debe entenderse la adquirida en ejercicio de las funciones propias de un empleo concreto o preciso, en el desempeño de actividades en una determinada área de trabajo o en el ejercicio profesional, o en el desempeño de una ocupación, arte u oficio, igual o similar al cargo, empleo o responsabilidad que se va a desempeñar.

PARÁGRAFO QUINTO: Además de las obligaciones generales a cargo de cada perfil, el personal mínimo requerido deberá realizar las funciones propias de la naturaleza del contrato, dando cumplimiento a la normatividad vigente y sus modificaciones.

PARÁGRAFO SEXTO: El contratista deberá contar con todo el personal técnico, profesional y administrativo que sea necesario para la correcta ejecución del contrato, sin que ello implique costos adicionales para el P.A. FONTUR.

PARÁGRAFO SÉPTIMO: En caso de requerirse algún cambio, por circunstancias de fuerza mayor o caso fortuito, de alguno de los miembros del personal mínimo requerido, la hoja de vida de la nueva persona o personas a cambiar deberá tener las mismas o mejores calidades (formación y experiencia), respecto a las condiciones establecidas dentro de los términos en el proceso de invitación abierta.

PARÁGRAFO OCTAVO: En los casos que se requiera experiencia profesional, la misma se contará a partir de la fecha de expedición del título profesional o de la tarjeta profesional o matrícula profesional (cuando aplique) según lo establecido para cada profesión. En caso de presentar profesionales graduados en el extranjero, la experiencia profesional se contará a partir de la fecha de grado, cuando en el país respectivo no emitan o no aplique la tarjeta profesional.

PARÁGRAFO NOVENO: Si el contratista, o integrante del grupo empresarial al que pertenezca el contratista, es quien emite la certificación del personal, para hacerla valer, deberá aportar como mínimo lo siguiente:

- Acuerdo contractual correspondiente suscrito entre el contratante y el profesional certificado,
- Planillas de pago de seguridad social,
- Recibos de pago,
- Otros documentos que permitan demostrar la relación contractual o laboral, y en donde conste que trabajaba o trabajó con ese contratante en el plazo certificado.

PARÁGRAFO DÉCIMO: Si la experiencia certificada se obtuvo en el marco del desarrollo de un proyecto, se deberá presentar el acuerdo contractual suscrito entre el contratante (la entidad pública o privada) y quien certifica, para verificar alcance y/o actividades principales del acuerdo contractual.

PARÁGRAFO DÉCIMO PRIMERO: Para las acreditaciones presentadas para los perfiles del personal clave que correspondan a cargos públicos (provisional, o de carrera administrativa, o de Libre Nombramiento y Remoción), podrán presentar la certificación en donde se evidencie el número de resolución de nombramiento y/o número acta de posesión y las actividades y/o funciones realizadas.

PARÁGRAFO DÉCIMO SEGUNDO: Si alguno de los elementos mínimos de información requeridos (objeto, alcance, actividades, inicio y fin de las actividades, entre otros), no se encuentra en la certificación aportada de los acuerdos contractuales, el contratista deberá anexar copia del acta de inicio, acta de liquidación, otrosíes o demás documentos contractuales respectivos, siempre y cuando, estos documentos contengan la información no incluida en la respectiva acreditación.

PARÁGRAFO DÉCIMO TERCERO: El contratista para la conformación del personal clave deberán tener en cuenta el porcentaje (%) de dedicación asignado a los mismos en las OBLIGACIONES ESPECIFICAS DEL CONTRATISTA de la minuta del contrato. Por consiguiente, el SUPERVISOR realizará internamente las verificaciones necesarias para determinar si ese mismo personal clave ha sido presentado en: i) procesos de Invitación Abierta que se encuentren en proceso de adjudicación, o que se encuentren adjudicados por el P.A. FONTUR, al momento de la solicitud de subsanables del presente proceso de selección o ii) que hagan parte de contratos que se encuentren vigentes y/o en ejecución en el P.A. FONTUR al momento de la solicitud de subsanables del presente proceso de selección. En caso de que se verifique, que, por ocasión de alguno de los eventos antes descritos, algún perfil no cuente con el porcentaje de dedicación exigido, el mismo no será tenido en cuenta para el presente proceso. En todo caso el SUPERVISOR realizará las solicitudes de subsanación o aclaraciones que correspondan.

PARÁGRAFO DÉCIMO CUARTO: Las auto certificaciones aportadas por el personal para acreditar su propia experiencia NO SERAN TENIDAS EN CUENTA. Sin embargo, esa experiencia podrá ser verificada por el P.A FONTUR y podrán ser tenida en cuenta, si con las certificaciones se aportan acuerdos contractuales o documentos emitidos por terceros, que demuestren la prestación del servicio o la ejecución de actividades que se deriven del mismo y que permitan evidenciar con claridad la información de la experiencia que se pretenda acreditar (fechas de inicio y terminación, actividades desarrolladas, etc.).

PARÁGRAFO DÉCIMO QUINTO: El desarrollo de las actividades a cargo del personal contemplará y cubrirá todos los costos y gastos logísticos que se requieran para su ejecución, los cuales estarán a cargo del contratista.

PARÁGRAFO DÉCIMO SEXTO: El P.A. FONTUR será eximido de cualquier responsabilidad con ocasión de las situaciones de riesgo y/u orden público por las que se pueda ver afectado el contratista y su personal.

TERCERA. TÉRMINO DE EJECUCIÓN: El plazo de ejecución del contrato será de **DOS (2) MESES** contados a partir de la aprobación de las garantías mediante la plataforma SECOP II. Es decir, el contratista tendrá este plazo para instalar conforme el anexo técnico las soluciones de seguridad perimetral requeridas.

Es pertinente indicar que los servicios de soporte, garantía y duración de las licencias será de **DOCE (12) MESES** contados a partir de la instalación y puesta en producción de las soluciones.

CUARTA. VALOR DEL CONTRATO: Para todos los efectos legales el valor del presente Contrato es hasta por la suma de XXXXXXXXX ($XXXXXX), incluido IVA, con cargo a los Documentos de Disponibilidad Presupuestal No. No. 346 del 3 de diciembre de 2025 (recursos fiscales) No. 631 del 3 de diciembre de 2025 (recursos parafiscales) y No. 319 del 20 de marzo de 2026 (recursos parafiscales), expedido por la Dirección de Presupuesto, Contabilidad y Operaciones del P.A. FONTUR

PARÁGRAFO PRIMERO: Todos los impuestos, tasas y retenciones que apliquen, así como aportes a seguridad social y demás gastos que se generen en la suscripción y ejecución del presente contrato, serán asumidos por EL CONTRATISTA.

4.1. Fuente de Recursos:

Fuente de Recursos	Número y Nombre del Proyecto	Documento de Disponibilidad Presupuestal (número y fecha)	Valor por Comprometer
FISCALES	NO APLICA	No. 346 del 3 de diciembre de 2025	$250.000.000
PARAFISCALES	NO APLICA	No. 631 del 3 de diciembre de 2025	$600.000.000
PARAFISCALES	NO APLICA	No. 319 del 20 de marzo de 2026	$231.285.204
TOTAL			$1.081.285.204

QUINTA. FORMA DE PAGO: El valor del contrato se pagará de la siguiente forma:

- FONTUR pagará al **CONTRATISTA** el valor total del contrato, en **UN (1) UNICO PAGO**, una vez hayan sido implementadas, puestas en producción y recibidas a satisfacción por parte del supervisor designado las soluciones y herramientas objeto del contrato, contra presentación de la correspondiente factura por parte del CONTRATISTA. El pago se realizará a la cuenta bancaria certificada por el contratista, dentro de los plazos y el cronograma estipulados por el contratante, pagaderos dentro de los 30 días siguientes a la presentación de la factura previa expedición del formato de recibido a satisfacción y autorización para el trámite de pago.

PARÁGRAFO PRIMERO: Para cada uno de los pagos **EL CONTRATISTA**, en caso de ser persona jurídica deberá presentar con la factura o cuenta de cobro (según sea el caso), la certificación del Revisor Fiscal o Representante Legal, donde indique que se encuentra al día en el pago de aportes al Sistema de Seguridad Social, Sena, ICBF, etc. En caso de persona natural, deberá presentar las planillas de pago de los aportes al Sistema de Seguridad Social.

PARÁGRAFO SEGUNDO: Si durante el plazo de ejecución del Contrato, **EL CONTRATISTA** presenta un cambio en su régimen tributario, lo deberá informar al supervisor y allegar los soportes respectivos, dentro de los diez (10) días siguientes a la identificación de este cambio. El cambio de régimen durante la ejecución del contrato no implica reconocimientos de sumas adicionales o modificaciones al valor del contrato, estos deberán ser asumidos por **EL CONTRATISTA**.

PARÁGRAFO TERCERO: Los pagos se efectuarán, mediante consignación a la cuenta que el contratista indicó al momento de la suscripción del presente contrato y previa ejecución de los trámites administrativos y presupuestales a que haya lugar por parte de FONTUR, descontando los valores correspondientes a impuestos y retenciones, de conformidad por lo ordenado por la Ley.

PARÁGRAFO CUARTO: El Supervisor deberá expedir el Informe de Supervisión y Gestión de Pago con todos los soportes requeridos.

PARÁGRAFO QUINTO: Las Partes convienen que el P.A. FONTUR podrá negar o aplazar el pago total o parcial de una factura o una cuenta de cobro (según corresponda) cuando se presente cualquiera de los siguientes eventos:

a. La obligación respectiva haya sido cancelada con anterioridad.
b. Se cite en forma incorrecta el NIT o el nombre del obligado al pago.
c. El contenido de la factura o de la cuenta de cobro no esté de acuerdo con las condiciones del Contrato.
d. La factura o la cuenta de cobro (según corresponda) cuenta de cobro presente enmendaduras, alteraciones o modificaciones en su contenido.
e. La factura o la cuenta de cobro (según corresponda) por fuera de los plazos de radicación del calendario de pagos establecido por el Patrimonio Autónomo FONTUR, al cual se acoge desde ahora EL CONTRATISTA.
f. La factura o la cuenta de cobro (según corresponda) sin el lleno de los requisitos que fije la ley o regulación tributaria.
g. Se pretenda el cobro de la factura o cuenta de cobro (según corresponda) por un tercero distinto del emisor, que no haya cumplido con el aviso previo o los demás requisitos de la Ley 1231 de 2008. Para que la factura pueda endosarse, el vendedor o emisor debe haber dejado constancia expresa de su intención en el título y sólo podrá endosarse una vez aceptado el título.
h. No se haya notificado al vocero del Patrimonio Autónomo FONTUR el endoso o negociación del título, para que incluya las anotaciones sobre los pagos parciales.
i. Reciba orden de autoridad competente que suspenda la circulación de la factura, o afecte los derechos relacionados con la misma o con el negocio causal que le dio origen.
j. No existan recursos líquidos para el pago, o sean insuficientes de acuerdo con las

disponibilidades del fideicomiso y en su caso la prelación de pagos establecida en la ley.

PARÁGRAFO SEXTO: La factura o cuenta de cobro (según sea el caso), deberá librarse a nombre del PATRIMONIO AUTÓNOMO FONDO NACIONAL DEL TURISMO – FONTUR * NIT No. 900.649.119-9. Radicar en
FONTUR, de acuerdo con las indicaciones que imparta el supervisor. El trámite solamente se hace sobre la factura electrónica debidamente transmitida por la DIAN al correo establecido para este fin o la cuenta de cobro presentada, según sea el caso.

PARÁGRAFO SÉPTIMO: El retraso en el pago no genera intereses de ninguna naturaleza a favor del contratista seleccionado y estará sujeto al Programa Anual Mensualizado de Caja – PAC del P.A. FONTUR.

SEXTA. AUTORIZACIÓN DE PAGOS: Para obtener la autorización del pago, la cual se tramitará ante la Unidad de Cumplimiento de Operaciones Financieras de **FONTUR**, **EL CONTRATISTA** deberá observar:

a. Que el pago esté precedido de la presentación del informe correspondiente previa aprobación del supervisor.
b. Que con la cuenta de cobro se presente constancia suscrita por el representante de **EL CONTRATISTA**, de estar al día con el cumplimiento del pago de los aportes al sistema de seguridad social integral y parafiscal.
c. Que los anteriores documentos deben contar con la aprobación de **FONTUR** y se debe adjuntar a la respectiva cuenta de cobro. Sin el cumplimiento de tales requisitos, la cuenta de cobro se tendrá como no presentada.
d. Si la cuenta de cobro no es radicada dentro de los primeros 23 días del mes o presenta inconsistencias, ésta será devuelta a **EL CONTRATISTA** y los términos para el pago sólo empezarán a contarse desde la fecha en que se radique la cuenta de cobro corregida.
e. Que todas las demoras que se presenten por estos conceptos serán de responsabilidad de **EL CONTRATISTA**, quien no tendrá derecho al pago de intereses o compensación de ninguna naturaleza.

SÉPTIMA: OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA: Para el desarrollo del contrato, el contratista deberá dar cumplimiento a las siguientes obligaciones específicas:

1. Ejecutar el contrato dando estricto cumplimiento a las especificaciones técnicas y demás condiciones establecidas por el P.A. FONTUR para la presente contratación.
2. Entregar dentro de los cinco (5) días hábiles siguientes al inicio de la ejecución del contrato el plan de trabajo, la matriz de riesgos y el cronograma (en formato Microsoft Project) al supervisor designado del contrato.
3. Realizar una reunión de *kickoff* dentro de los seis (6) días hábiles siguientes al inicio de la ejecución del contrato para verificar y aprobar por parte de supervisor designado el plan de trabajo, la matriz de riesgos y el cronograma de implementación de la solución.

4. Realizar los informes solicitados con base en el modelo suministrado por el Patrimonio en donde se haga seguimiento al plan de trabajo, matriz de riesgos, cronograma y demás aspectos que la supervisión considere pertinentes.
5. Entregar las soluciones y herramientas objeto del contrato en el plazo establecido de ejecución del contrato según lo indicado en las especificaciones técnicas.
6. Entregar los licenciamientos a que haya lugar en los términos establecidos en las condiciones del proceso.
7. Garantizar las vigencias de soporte, mantenimiento y garantía de las soluciones objeto del contrato según lo indicado en las especificaciones técnicas.
8. El contratista deberá realizar la implementación, configuración, pruebas, integración con la infraestructura actual de P.A. FONTUR y la puesta en funcionamiento de las soluciones y herramientas contratadas conforme a las condiciones de las especificaciones técnicas.
9. Informar al supervisor del contrato de cualquier eventualidad que dificulte su ejecución, así como también deberá atender los requerimientos efectuados por el supervisor y en especial cualquier inquietud que pueda presentarse durante la implementación y puesta en funcionamiento de los productos adquiridos.
10. El contratista deberá atender directamente solicitudes de soporte por incidentes vía web, correo electrónico, chat y teléfono durante la implementación y puesta en producción de las soluciones y herramientas adquiridas. Durante el periodo de garantía, soporte y mantenimiento las solicitudes deberán ser respondidas por el fabricante conforme a las especificaciones técnicas establecidas.
11. Atender los requerimientos efectuados por el supervisor del contrato, y en especial cualquier inquietud que pueda presentarse durante la instalación y puesta en funcionamiento de los productos adquiridos.

OCTAVA. OBLIGACIONES GENERALES DEL CONTRATISTA: **EL CONTRATISTA** se obliga a:

1. Cumplir con los términos descritos en las cláusulas de: objeto, obligaciones y demás específicas técnicas contenidas en los documentos del proceso de Invitación Abierta y en la propuesta presentada.
2. Garantizar la oportuna, eficaz y eficiente prestación del servicio contratado y responder por su calidad.
3. Atender las indicaciones y orientaciones expuestas por el supervisor del contrato en cuanto a la ejecución de este.
4. Mantener en forma permanente, altos niveles de eficiencia técnica y profesional para atender sus obligaciones, garantizando criterios de idoneidad y experiencia.
5. Velar por la custodia de los documentos físicos y/o magnéticos que le sean entregados por la supervisión o que elabore en ejecución del contrato; y devolverlos a la terminación de la actividad contratada.
6. Informar por escrito a la supervisión, tan pronto tenga conocimiento de cualquier evento o situación que pueda afectar la normal ejecución del contrato.
7. Manejar con el debido respeto y confidencialidad la información a la que tenga acceso en desarrollo de sus actividades o con ocasión del presente contrato.
8. Presentar los informes de la ejecución contractual y en la periodicidad requerida en el contrato y por el supervisor del mismo.
9. Presentar al Supervisor del contrato dentro de los cinco (05) días siguientes a la terminación de éste, el informe final de actividades respecto del cumplimiento de

las actividades y obligaciones contractuales, con todos los soportes que le sean requeridos por el mismo.

10. Emplear los logos y realizar las menciones del Fondo Nacional de Turismo – P.A. FONTUR y del Ministerio de Comercio, Industria y Turismo en todos los productos y actividades que se realicen en la ejecución del contrato, con las autorizaciones correspondientes de imagen por parte del P.A. FONTUR.
11. Mantener y garantizar la afiliación al Sistema de Seguridad Social en Salud, Pensión y ARL, y estar al día en el pago de parafiscales, en caso de estar obligado por las leyes vigentes.
12. Constituir las garantías exigidas y aquellas necesarias para la legalización del contrato y mantenerlas vigentes durante la duración del mismo, incluidas las novedades contractuales.
13. Asumir todos los gastos de viaje, desplazamientos, viáticos y manutención de su personal en la ciudad donde se deberán prestar los servicios.
14. Participar en las reuniones que convoque el supervisor del contrato para la coordinación de actividades, y las demás que se consideren pertinentes.
15. Cumplir con las demás instrucciones relacionadas con el objeto del contrato que le sean impartidas por el supervisor del mismo.
16. Todas las demás que se desprendan de la naturaleza de este contrato, necesarias para su cumplimiento.

NOVENA. OBLIGACIONES DE FONTUR: **FONTUR** se obliga a:

1. Efectuar el pago en los términos establecidos en el presente Contrato.
2. Ejercer los controles necesarios para la cabal ejecución del Contrato.
3. Prestarle toda la colaboración a **EL CONTRATISTA** para que obtenga la información necesaria con la finalidad de que el objeto del Contrato se desarrolle.
4. Informar a **EL CONTRATISTA** de cualquier situación que se presente y de la cual se pueda percatar, que impida el normal desarrollo de las actividades propias del Contrato en materia financiera, técnica, jurídica, entre otras.
5. Todas aquellas que se desprendan de la naturaleza de este Contrato, necesarias para su cabal cumplimiento.

DÉCIMA PRIMERA. GARANTÍAS. EL CONTRATISTA, deberá otorgar a favor del Patrimonio Autónomo Fondo Nacional del Turismo – FONTUR con NIT. 900.649.119-9, una póliza expedida por una Compañía de Seguros legalmente establecida en Colombia y vigilada por la Superintendencia Financiera, en formato a favor de entidades particulares, que garantice los siguientes amparos:

a) **Cumplimiento del Contrato:** Por un valor asegurado equivalente al veinte por ciento (20%) del valor total del contrato, con una vigencia igual a su plazo, de sus prórrogas si las hubiere, y por doce (12) meses más.

NOTA: En todo caso, este amparo deberá cubrir el tiempo de garantía, soporte y mantenimiento que oferte el adjudicatario durante el proceso de selección.

b) **Calidad del servicio:** Por un valor asegurado equivalente al veinte por ciento (20%) del valor total del contrato, con una vigencia igual a su plazo, y de sus

prórrogas si las hubiere, y un (1) año más desde la suscripción del acta de recibo a satisfacción de los bienes o servicios suministrados.

PARÁGRAFO PRIMERO: Las garantías deberán ser publicadas por **EL CONTRATISTA** y aprobadas por la entidad a través de la plataforma SECOP II, estás deberán cargarse con el recibo de pago de la prima, así como con las condiciones generales.

La póliza deberá entregarse con el recibo de pago de la prima o su equivalente, así como con las condiciones generales de la misma dentro de los cinco (5) días hábiles siguientes a la suscripción del Contrato. **FONTUR** aprobará las pólizas si las encuentra ajustadas a lo especificado, en caso contrario, requerirá al Contratista para que dentro del plazo que **FONTUR** le señale, haga las modificaciones y aclaraciones necesarias.

PARÁGRAFO SEGUNDO: en caso de que la póliza tenga algún deducible, este será asumido por **EL CONTRATISTA. EL CONTRATISTA** deberá reponer el valor de las garantías cuando su valor sea afectado por razón de siniestros.

PARÁGRAFO TERCERO: en caso de modificaciones (suspensiones, reinicios, etc.) del Contrato, **EL CONTRATISTA**, se obliga a realizar los ajustes correspondientes a los amparos de las pólizas contempladas en esta cláusula, en caso de no remitir la actualización esto constituirá un presunto incumplimiento.

DÉCIMA PRIMERA. PROPIEDAD INTELECTUAL, DERECHOS DE AUTOR, Y DERECHOS PATRIMONIALES: FONTUR será el propietario exclusivo de los estudios, diseños, análisis, informes, documentos, aplicaciones, bases de datos, hardware, software y, en general, cualquier obra susceptible de protección por el derecho de autor, los signos distintivos como las marcas, enseñas y nombres comerciales, los modelos de utilidad, diseños industriales, las patentes, know how, secretos empresariales, invenciones, descubrimientos y demás intangibles considerados como **PROPIEDAD INTELECTUAL** que resulten de las actividades de **EL CONTRATISTA** en ocasión a la ejecución del presente Contrato.

En virtud de este Contrato, **EL CONTRATISTA** cede exclusivamente a FONTUR la totalidad de los derechos patrimoniales de autor sobre las Obras susceptibles de protección por el derecho de autor, sin remuneración adicional a la pactada en el presente **CONTRATO**. La cesión de los derechos patrimoniales de autor será para todos los medios y formatos conocidos y por conocerse, incluyendo, pero sin limitarse a análogo y digital, y tendrá efectos en todos los países del mundo, por el término de protección de cada Obra que sea objeto de esta Cláusula.

Las Obras susceptibles de protección por el derecho de autor quedarán exclusivamente a **FONTUR**. FONTUR entiende que los derechos morales de autor son irrenunciables, conforme a lo consagrado en la Ley 23 de 1982, modificada por la Ley 1450 de 2011. En todo caso, FONTUR respetará los derechos morales de autor, realizando las menciones correspondientes en la bandera editorial de las publicaciones, cuando corresponda.

EL CONTRATISTA autoriza a **FONTUR** para registrar los intangibles y Obras ante las Autoridades Competentes, y se compromete a tomar las acciones necesarias y a suministrar todos los documentos requeridos para este fin.

EL CONTRATISTA entiende y acepta que **FONTUR** queda facultado, sin limitación alguna, para efectuar, entre otras, las siguientes acciones: reproducción a través de cualquier medio físico o digital de las obras, la distribución de copias de las obras en favor de terceros, la comunicación pública o puesta a disposición del público de las obras a través de cualquier medio análogo o digital, la transformación de la obra bien sea alterando su formato original, traduciéndola a otros idiomas o en cualquier otro sentido, la comercialización de la obra, el uso en redes sociales, aplicaciones web de acceso por vía internet o descargables, páginas web, enlaces, interfaces de usuario o medios análogos y tradicionales; sobre los bienes intangibles, Obras y derechos que se adquieren a en virtud de esta Cláusula.

PARÁGRAFO PRIMERO: Las **PARTES** declaran que conocen y entienden las normas relativas a la propiedad intelectual y se comprometen a cumplirlas durante la ejecución del presente Contrato y con posterioridad a su terminación, especialmente en relación con los intangibles que estén en cabeza de cada una de las **PARTES** con anterioridad a la celebración del Contrato.

PARÁGRAFO SEGUNDO: Serán de exclusiva titularidad de **EL CONTRATISTA**, las obras científicas, artísticas y literarias (entre estas los programas informáticos o software) que hubiera creado con anterioridad a la celebración del Contrato, así como los bienes intangibles que fueran de su propiedad con anterioridad a la celebración del Contrato. En todo caso, **EL CONTRATISTA** autoriza a **FONTUR** el uso, comunicación pública, reproducción, transformación, explotación y, el ejercicio de cualquier otro derecho patrimonial de autor existente sobre las Obras **de EL CONTRATISTA** creadas con anterioridad a la celebración del Contrato y que hayan sido empleadas durante la ejecución de este y/o se encuentren dentro de los entregables de éste. La autorización aplicará para todos los medios y formatos conocidos y por conocerse, durante todo el término de la protección legal y para todos los países del mundo. FONTUR a su vez está plenamente facultado para autorizar a terceros el uso de las Obras **de EL CONTRATISTA** creadas con anterioridad a la celebración del Contrato.

Por su parte, las obras científicas, artísticas y literarias, así como los signos distintivos y demás intangibles de **FONTUR** que sean expuestos o que se pongan a disposición de **EL CONTRATISTA** con ocasión de este Contrato, serán de exclusiva titularidad de FONTUR.

Ninguna de las **PARTES** podrá explotar, distribuir, reproducir, comunicar, alterar, y en general, usar las Obras o bienes intangibles de propiedad de la otra PARTE por fuera de los términos del Contrato, sin previa autorización. La única excepción a este inciso será el inciso Primero del **PARÁGRAFO SEGUNDO** de la presente cláusula.

PÁRAGRAFO TERCERO: Esta Cláusula será aplicable a cualquier derecho de propiedad intelectual que surja en virtud de la actividad de **EL CONTRATISTA** en ocasión de este Contrato.

PARÁGRAFO CUARTO: EL CONTRATISTA declara que es titular de los derechos patrimoniales de autor sobre las Obras que autoriza o cede en virtud de esta Cláusula, y garantiza que en su creación o desarrollo no se infringieron derechos de terceros. por lo que, se compromete a mantener libre e indemne a **FONTUR** de cualquier daño o

perjuicio originado por reclamaciones o litigios iniciados por terceros en relación con la titularidad de los derechos que son autorizados y/o cedidos mediante el presente Contrato.

EL CONTRATISTA declara que realizó todas las gestiones encaminadas a garantizar la completa titularidad sobre las Obras, a favor **FONTUR. EL CONTRATISTA** obtuvo todas las cesiones correspondientes por parte de los autores que participaron en el desarrollo las Obras, las cuales se entregan a FONTUR, junto con la firma del Contrato. Asimismo, se obliga a obtener y a aportar los documentos que sean necesarios para la cesión a **FONTUR** de los derechos que pueda tener sobre los intangibles y/o las Obras que surjan de la ejecución del Contrato, incluyendo, pero sin limitarse, los contratos de trabajo, de prestación de servicios o de cesión, y las autorizaciones o releases requeridos para asegurar la titularidad de **FONTUR** sobre éstos. Adicionalmente, aportará la expresa declaración de su autoría sobre las Obras.

PARÁGRAFO QUINTO: EL CONTRATISTA manifiesta que las Obras objeto de la autorización y/o cesión a través del presente Contrato son y/o serán originales y fueron y/o serán realizadas por éste sin violar, usurpar, copiar, modificar, o en general atentar contra derechos de autor de terceros. Por lo tanto, en caso de presentarse cualquier reclamación o acción por parte de un tercero, **EL CONTRATISTA** asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados y cedidos y de **FONTUR**.

DÉCIMA SEGUNDA. BUENA FE Y LEALTAD NEGOCIAL. Dentro de la relación contractual las partes se comprometen a actuar de acuerdo con los postulados de buena fe y lealtad negocial. Las partes no podrán limitar este deber de carácter imperativo.

DÉCIMA TERCERA. INEXISTENCIA DE RELACIÓN LABORAL. EL CONTRATISTA y **FONTUR**, manifiestan que el presente Contrato es de naturaleza civil y por consiguiente no existe con ocasión a la ejecución del objeto del presente Contrato relación de carácter permanente o continuado, ni subordinación ni dependencia alguna, llámese ésta técnica, personal, económica o simplemente jurídica, y así lo declaran y estipulan las Partes. Los servicios contratados se ejecutarán de manera autónoma y sin subordinación, razón por lo cual no genera relación laboral ni prestaciones sociales y ningún tipo de costos distintos al valor acordado en la Cláusula Séptima del presente negocio jurídico.

DÉCIMA CUARTA. SUSPENSIÓN DEL CONTRATO. De común acuerdo las partes, **FONTUR** y **EL CONTRATISTA**, previa solicitud y visto bueno Supervisor del Contrato, podrán suspender la ejecución del Contrato para lo cual suscribirán un acta en donde se indicará la razón de la suspensión del Contrato; el término de duración de esta y la fecha de su reanudación.

DÉCIMA QUINTA. CESIÓN DEL CONTRATO. EL CONTRATISTA NO podrá ceder el Contrato salvo autorización expresa y previa de **FONTUR**. **EL CONTRATISTA** acepta incondicionalmente la cesión del Contrato que **FONTUR** deba realizar al Ministerio de Comercio, Industria y Turismo o la entidad que éste designe.

DÉCIMA SEXTA. TERMINACIÓN DEL CONTRATO. El Contrato podrá darse por terminado en cualquiera de los siguientes eventos:

1. Por disolución del **CONTRATISTA**.
2. Por mutuo acuerdo de las Partes.
3. Por incumplimiento de las obligaciones de cualquiera de las partes, previa evaluación del Supervisor del Contrato.
4. Cuando la ejecución de las obligaciones contenidas en el Contrato se desarrolle en forma tal que no garantice razonablemente la correcta ejecución de su objeto.
5. Por vencimiento del término inicialmente pactado.
6. En caso de incurrirse en una inhabilidad, incompatibilidad o conflicto de interés no advertida al momento de contratar o corresponda a un hecho sobreviniente.
7. En caso de que algún ente de control determine que los hechos objeto de la indagación al Representante Legal culminen en una sanción o sean determinados posteriormente como un delito de orden penal u otro, y por ende se genere culpabilidad o inhabilidad en el actual representante legal a quien se le encontró la coincidencia.
8. De manera unilateral por el P.A FONTUR, informándole al CONTRATISTA con quince (15) días de antelación.
9. Por las demás causales establecidas en el contrato.

DÉCIMA SÉPTIMA. EJECUCIÓN PARCIAL DEL CONTRATO. Si el Contrato se ejecuta en forma parcial, el valor de este se liquidará en proporción a la parte efectivamente ejecutada.

DÉCIMA OCTAVA. INCUMPLIMIENTOS LEVES (INCLUYE APREMIOS SI APLICA): Son los incumplimientos contractuales atribuibles al contratista que se presentan durante el plazo de ejecución del contrato con un carácter subsanable, que no afectan gravemente la continuidad contractual, pero que pueden causar retardos injustificados o cuando se incumplen actividades subsidiarias de la actividad principal que no permiten la debida vigilancia y corroboración del cumplimento del objeto contractual. FONTUR, llevará a cabo el proceso de incumplimiento leve de acuerdo con las causales y el procedimiento definido dentro del Manual de Contratación de FONTUR que se encuentra debidamente publicado en su página web y que el contratista declara conocer.

DÉCIMA NOVENA. REQUERIMIENTO POR INCUMPLIMIENTO IMPUTABLE AL CONTRATISTA DE UN ACUERDO DE SERVICIO (SI APLICA). En caso de incumplimiento imputable al **CONTRATISTA** de cualquiera de los acuerdos de servicio de los que trata la cláusula anterior, el supervisor del Contrato remitirá al **CONTRATISTA** un REQUERIMIENTO por escrito dentro de los tres (3) días hábiles siguientes al momento en que conoció los hechos, mediante el que: (i) informará dicha situación, (ii) indicará las acciones de mejora o correctivas necesarias y (iii) establecerá el término dentro del cual se deben realizar dichas acciones por parte de **EL CONTRATISTA** para solucionar el presunto incumplimiento. De dicho requerimiento se deberá dar traslado al área técnica responsable del Contrato y remitir copia de dicho informe a la FIDUCIARIA vocera y administradora de **FONTUR** y a la Compañía Aseguradora correspondiente. El supervisor deberá realizar el seguimiento a las acciones de mejora y correctivas planteadas.

VIGÉSIMA. PENALIDAD POR INCUMPLIMIENTO DE LOS ACUERDOS DE SERVICIO (SI APLICA). En caso de incumplimiento total o parcial, o cumplimiento defectuoso, por parte de **EL CONTRATISTA,** de lo dispuesto en el REQUERIMIENTO

formulado por el supervisor al **CONTRATISTA**, éste pagará a **FONTUR** un valor equivalente a un porcentaje de **entre 0.1% y 5%** del valor del Contrato, que será determinado por el porcentaje que se haya establecido de manera previa en el acuerdo de servicio a que hace referencia esta cláusula, para el incumplimiento de este. Esta suma será exigible ejecutivamente con la simple demostración del incumplimiento del REQUERIMIENTO formulado respecto del acuerdo de servicio incumplido con anterioridad, y se hará mediante informe expedido por el supervisor del Contrato que deberá ser suficientemente descriptivo frente a los hechos y circunstancias que originaron el incumplimiento y/o retraso de los acuerdos de servicios, y que deberá ser comunicado al **CONTRATISTA**, a la Presidencia de **FONTUR**, y al área técnica responsable del Contrato.

PARÁGRAFO PRIMERO: el mecanismo para el cobro por parte de **FONTUR** del valor que se genere por la aplicación de la presente cláusula será, preferiblemente, el establecido en el PARÁGRAFO CUARTO.

PARÁGRAFO SEGUNDO: en ningún caso el pago derivado del cobro de la obligación contenida en esta cláusula tendrá como efecto la extinción de la obligación principal del Contrato, ni de ninguna otra obligación que se haya estipulado dentro del mismo. En ese entendido, se podrá exigir por parte de **FONTUR** de manera simultánea el cumplimiento de la obligación principal, o cualquiera otra del Contrato, y el pago de la suma de dinero determinada en virtud de lo dispuesto en la presente cláusula.

PARÁGRAFO TERCERO. el cobro por parte de **FONTUR** de la obligación contenida en esta cláusula no excluye la posibilidad que tiene **FONTUR** de perseguir la indemnización de perjuicios a que tenga derecho por el incumplimiento contractual en que haya incurrido **EL CONTRATISTA**. En ese entendido, el cobro coactivo de la obligación contenida en la presente cláusula no excluye de ninguna manera, la aplicación de la **TASACIÓN ANTICIPADA DE PERJUICIOS POR INCUMPLIMIENTO DEL OBJETO CONTRACTUAL** o de la **PENALIDAD POR INCUMPLIMIENTO DEL OBJETO CONTRACTUAL**, contenidas en las cláusulas subsiguientes del presente documento.

PARÁGRAFO CUARTO: en cualquier caso, **FONTUR** podrá compensar (mediante la realización de descuentos y/o deducciones), de conformidad con lo establecido por los artículos 1714 a 1723 del Código Civil, hasta la concurrencia de los valores que se adeuden a **EL CONTRATISTA** por cualquier concepto, incluso respecto de Contratos diferentes al que se suscribe en el presente documento.

PARÁGRAFO QUINTO: la obligación contenida en la presente cláusula presta mérito ejecutivo una vez cumplida la condición de la que se supedita su nacimiento y exigibilidad, por tratarse en ese momento de una obligación clara, expresa y actualmente exigible.

VIGÉSIMA PRIMERA. PRESENTACIÓN POR PARTE DEL CONTRATISTA DE UN PLAN DE MEJORAMIENTO (SI APLICA). Una vez aplicada al **CONTRATISTA** la penalidad establecida en la Cláusula anterior, **EL CONTRATISTA** deberá presentar, para aprobación del supervisor del Contrato, un PLAN DE MEJORAMIENTO que permita normalizar la ejecución contractual. El supervisor del Contrato realizará el seguimiento de dicho PLAN DE MEJORAMIENTO.

VIGÉSIMA SEGUNDA. CLÁUSULA PENAL POR INCUMPLIMIENTO DEL OBJETO CONTRACTUAL -TASACIÓN ANTICIPADA DE PERJUICIOS-. En caso de incumplimiento total o cumplimiento defectuoso, por parte del **CONTRATISTA** del objeto del Contrato, **EL CONTRATISTA** pagará a **FONTUR**, a título de cláusula penal con función **de tasación anticipada de perjuicios**, una pena equivalente al **TREINTA POR CIENTO (30%)** del valor total del Contrato. Esta suma será exigible ejecutivamente con la simple demostración del incumplimiento de las obligaciones contractuales, para lo cual deberán observarse el siguiente procedimiento:

1. El supervisor del Contrato emitirá Informe de incumplimiento, explicando los hechos y razones que sustentan el incumplimiento del **CONTRATISTA** y el contenido mínimo señalado en el Manual de Contratación. Este informe deberá ser puesto en conocimiento del **CONTRATISTA** y de **FONTUR**, dejando constancia de este y otorgando un plazo prudencial de cinco (05) días hábiles para que **EL CONTRATISTA** se pronuncie, y si lo estima conveniente, plantee fórmulas de subsanación del incumplimiento. La notificación de este informe constituye en mora al **CONTRATISTA** en relación con la obligación incumplida, si ello no hubiere ocurrido antes por advenimiento de un término.

2. Una vez recibida la respuesta del **CONTRATISTA**, **FONTUR** podrá establecer el incumplimiento e imponer la cláusula penal si lo considera conveniente, y así deberá notificarlo al **CONTRATISTA** explicando detalladamente en qué consiste el incumplimiento, procediendo a ordenar el inicio del proceso de siniestralidad de la garantía por los perjuicios a que hubiere lugar y/o procediendo con las acciones legales correspondientes cuando lo estime procedente, de conformidad con lo estipulado en el Manual de Contratación del P.A. FONTUR.

PARÁGRAFO PRIMERO. En ningún caso el pago de la obligación contenida en esta cláusula penal tendrá como efecto la extinción de la obligación principal del Contrato, ni de ninguna otra obligación que se haya estipulado dentro del mismo. En ese entendido, se podrá exigir por parte de **FONTUR** de manera simultánea el cumplimiento de la obligación principal, o cualquiera otra del Contrato, y el pago de la suma de dinero estipulada en la presente cláusula penal pecuniaria.

PARÁGRAFO SEGUNDO. El cobro por parte de **FONTUR** de la obligación contenida en esta cláusula penal no excluye la posibilidad que tiene **FONTUR** de perseguir la indemnización de perjuicios a que tenga derecho por el incumplimiento contractual en que haya incurrido **EL CONTRATISTA.**

PARÁGRAFO TERCERO. En cualquier caso, **FONTUR** podrá compensar (mediante la realización de descuentos y/o deducciones), de conformidad con lo establecido por los artículos 1714 a 1723 del Código Civil, el valor de esta cláusula penal, hasta la concurrencia de los valores que se adeuden al **CONTRATISTA** por cualquier concepto, incluso respecto de Contratos diferentes al que se suscribe en el presente documento. Esta condición es aceptada de manera expresa por el **CONTRATISTA** con la suscripción del contrato.

PARÁGRAFO CUARTO. La presente cláusula penal no constituye una renuncia por parte de **FONTUR** a la posibilidad de perseguir la indemnización de los perjuicios que le sean

causados con ocasión del incumplimiento por parte del **CONTRATISTA** de la CLÁUSULA PRIMERA del Contrato, y cuya cuantía exceda el monto pactado en la presente cláusula a título de tasación anticipada de perjuicios. Dicha indemnización podrá ser exigida por **FONTUR** mediante las acciones judiciales que la Ley le confiere para tal efecto.

PARÁGRAFO QUINTO. La obligación contenida en la presente cláusula penal presta mérito ejecutivo una vez cumplida la condición de la que se supedita su nacimiento y exigibilidad, por tratarse en ese momento de una obligación clara, expresa y actualmente exigible.

VIGÉSIMA TERCERA. SUPERVISIÓN. La supervisión estará a cargo de un Profesional de la Oficina de Tecnología del P.A. FONTUR, que ejercerá las labores de supervisión conforme a lo establecido en los Manuales de Contratación y de Supervisión del P.A FONTUR, quien haga sus veces, o quien designe el Representante Legal del P.A. FONTUR para tal efecto. Además de las obligaciones establecidas en sus contratos, deberá realizar las siguientes actividades:

1. Colaborar con **EL CONTRATISTA,** para una cabal ejecución del presente contrato.
2. Exigir y vigilar que el contrato se desarrolle de acuerdo con las cláusulas contractuales.
3. Atender y resolver las consultas planteadas por **EL CONTRATISTA** para el buen desarrollo del objeto del contrato.
4. Comunicar con la debida oportunidad cualquier situación que afecte la normal ejecución del objeto contractual.
5. Velar y exigir a **EL CONTRATISTA** que dé cumplimiento a la expedición de las modificaciones requeridas de las pólizas que fueron exigidas en el presente contrato, en especial en lo referente a los procedimientos de cesión que sufra el contrato.
6. Certificar que **EL CONTRATISTA** cumplió con las obligaciones contenidas en la Cláusula de Obligaciones de **EL CONTRATISTA** del presente contrato.
7. Estudiar y recomendar cambios sustanciales al proyecto presentado que sean convenientes o necesarios.
8. Decidir sobre cambios propuestos por **EL CONTRATISTA** al proyecto, siempre que no afecten la correcta ejecución del objeto contratado.
9. Aprobar o rechazar, en forma debidamente motivada, los procedimientos utilizados para la ejecución del objeto contratado y rendir informes sobre el desarrollo del objeto del mismo.
10. Suscribir las actas de inicio y recibo definitivo que se exijan en el contrato, conjuntamente con **EL CONTRATISTA.**
11. Suscribir las actas de suspensión y reinicio cuando fuere el caso, conjuntamente con **EL CONTRATISTA**, situaciones de las cuales rendirá informe al **FONTUR**.
12. Presentar Informes mensuales sobre la ejecución y cumplimiento del Contrato.
13. Presentar a la finalización del contrato un informe sobre la ejecución y cumplimiento del contrato. La presentación del informe del supervisor es requisito indispensable para el pago a **EL CONTRATISTA**.
14. Las demás funciones que se consideren necesarias para el cabal cumplimiento del objeto del contrato o que se deriven del mismo.

PARÁGRAFO PRIMERO. Las instrucciones impartidas en el ejercicio de tales funciones deberán constar por escrito. Las dadas en forma verbal, por urgencia o necesidad inminente, deberán ratificarse por escrito. La presentación del informe del supervisor es requisito indispensable para realizar el (los) pago(s) a **EL CONTRATISTA**.

VIGÉSIMA CUARTA. SOLUCIÓN DE CONTROVERSIAS. Las partes convienen resolver de manera directa, y de común acuerdo cualquier diferencia que surja entre ellas con ocasión de la ejecución, la interpretación y el alcance del Contrato. En caso de no lograrse resolver la controversia de manera directa, las partes podrán acordar mediante documento debidamente suscrito, el mecanismo escogido para la resolución de las controversias contractuales, tales como: conciliación, transacción, amigable composición, en caso de no llegarse a algún acuerdo, las partes quedan en plena libertad de acudir a la jurisdicción ordinaria. Lo anterior sin perjuicio de la facultad del **P.A. FONTUR** de declarar el incumplimiento del Contrato.

PARÁGRAFO PRIMERO: en caso de que las partes opten por el mecanismo de resolución controversias ante un centro de conciliación, los gastos que este trámite genere correrán por cuenta de los involucrados en la controversia en partes iguales.

PARÁGRAFO SEGUNDO: en caso de que las partes opten por el mecanismo de resolución de controversias ante un amigable componedor, los gastos que ocasionen por este concepto serán cubiertos, en principio, por partes iguales entre los involucrados en la controversia. Una vez tomada la decisión por el Amigable Componedor, los gastos los asumirá la parte que resulte vencida. Culminada la amigable composición, las partes harán los reembolsos de gastos por la intervención del Amigable Componedor. En caso en que no resulte evidente cuál es la parte vencida frente a este mecanismo de solución de controversias, será el amigable componedor quien decida, sobre este aspecto.

VIGÉSIMA QUINTA. AUTORIZACIÓN, REPORTE Y CONSULTA A TRASUNIÓN. AUTORIZACIÓN EXPRESA PARA REPORTAR, CONSULTAR Y COMPARTIR INFORMACIÓN CONTENIDA EN LAS BASES DE DATOS FINANCIERA, CREDITICIA, COMERCIAL, DE SERVICIOS Y LA PROVENIENTE DE OTROS PAÍSES. EL CONTRATISTA autoriza expresa e irrevocablemente a **FONTUR,** libre y voluntariamente, para que reporte a TRASUNIÓN, o a cualquier otro operador legalmente establecido, toda la información que refleje su comportamiento como cliente que se relacione con el nacimiento, ejecución, modificación, liquidación y/o extinción de las obligaciones que se deriven del Contrato. La permanencia de la información estará sujeta a los principios, términos y condiciones consagradas en la Ley 1266 de 2008, Ley 1581 de 2012, y demás normas que la modifiquen, aclaren o reglamenten. Así mismo**, EL CONTRATISTA** autoriza, expresa e irrevocablemente a **FONTUR,** para que consulte toda la información financiera, crediticia, comercial, de servicios y la proveniente de otros países, atinente a sus relaciones comerciales que él tenga con el sistema financiero, comercial y de servicios, o de cualquier sector, tanto en Colombia como en el exterior, con sujeción a los principios, términos y condiciones consagrados en la citada Ley y demás normas que la modifiquen, aclaren o reglamenten.

VIGÉSIMA SEXTA. RIESGO DE LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA: EL CONTRATISTA: El **CONTRATISTA** se compromete a adoptar medidas para prevenir y

controlar el riesgo de lavado de activos, la financiación al terrorismo y proliferación de armas de destrucción masiva en su organización y en desarrollo de todas sus relaciones, entre ellas las laborales, comerciales y corporativas. De esta manera, el **CONTRATISTA** responderá a la **CONTRATANTE** indemnizándole por cualquier multa o perjuicio que se le cause a la **CONTRATANTE** y que tenga como origen el incumplimiento de los compromisos antes expresados.

EL CONTRATISTA certifica al Contratante que sus recursos no provienen ni se destinan al ejercicio de ninguna actividad ilícita, entre ellas, las conductas tipificadas como delitos fuente de lavado de activos y financiación del terrorismo. Así mismo, se obliga a realizar todas las actividades encaminadas a asegurar que sus administradores, socios, beneficiarios finales, empresas vinculadas en cualquier de los eventos de los artículos 26, 27 y 28 de la Ley 222 de 1995, inversionistas y donantes, y los recursos de éstos, no se encuentren relacionados o provengan de actividades ilícitas entre ellas, las conductas tipificadas como delitos fuente de lavado de activos y financiación del terrorismo.

En dicho sentido, **EL CONTRATANTE** podrá dar por terminado el presente contrato si en su ejecución, por cualquier medio tiene conocimiento que:

- **EL CONTRATISTA**, o algunos de sus administradores, socios, beneficiarios finales, empresas vinculadas en cualquier de los eventos de los artículos 26, 27 y 28 de la Ley 222 de 1995, inversionistas, o donantes, llegaren a resultar inmiscuidos en una investigación de cualquier tipo (penal, administrativa, etc.) relacionada con conductas tipificadas como delitos fuente de lavado de activos y financiación del terrorismo, o fuesen incluidos en listas vinculantes LAFT
- Por decretarse respecto al **CONTRATISTA** el desmonte de operaciones, o la intervención para administración o la liquidación por autoridad competente por actividades de captación ilegal de recursos o de extinción del derecho de dominio.
- EL **CONTRATISTA** o alguno de sus administradores o socios se encuentren vinculados con formulación de acusación a conductas tipificadas como delitos fuente de lavado de activos y financiación del terrorismo o se encuentren reportados por algún órgano de inspección, vigilancia o control u organismo judicial, por conductas asociadas a presunto lavado de activos y/o financiación del terrorismo.
- Cuando existan factores de exposición al riesgo tales como: referencias negativas con relación al **CONTRATISTA** alguno de sus administradores, socios, beneficiarios finales, empleados, empresas vinculadas en cualquier de los eventos de los artículos 26, 27 y 28 de la Ley 222 de 1995, inversionistas, donantes, adherentes, o la configuración de las alertas enumeradas en las políticas y procedimientos del SARLAFT de la FIDUCIARIA.

En consecuencia, una vez acaecido alguno de los eventos descritos anteriormente la **CONTRATANTE** mediante comunicación dirigida al **CONTRATISTA**, a su última dirección física y/o último correo electrónico registrado, informará la terminación y liquidación del contrato, sin que por este hecho esté obligado a indemnizar de ningún tipo de perjuicio al **CONTRATISTA**.

Así mismo, **LA CONTRATANTE** estará facultada para suspender todos los pagos o giros que de conformidad con el contrato deban efectuarse con ocasión al acaecimiento del referido evento.

PARÁGRAFO PRIMERO - ACTUALIZACIÓN DE INFORMACIÓN: El **CONTRATISTA** se obliga a actualizar dentro de la periodicidad establecida por la **FIDUCIARIA** o cuando esta última lo requiera, la información necesaria para el cumplimiento de las disposiciones del Sistema de Administración de Riesgo del Lavado de Activos y Financiación del Terrorismo – SARLAFT, así como suministrar los soportes documentales necesarios para confirmar los datos. No obstante, lo anterior, **EL CONTRATISTA** autoriza expresamente a FIDUCOLDEX, mediante la suscripción del presente Contrato, para que ésta contrate con terceros locales o extranjeros, servicios relacionados con el procesamiento de datos para su utilización en servicios de atención telefónica para la actualización de información u otras de naturaleza similar, garantizando en todo caso, la confidencialidad de la información que le asiste y a la que está obligada la FIDUCOLDEX.

PARÁGRAFO SEGUNDO: En todo caso, **EL CONTRATISTA** se obliga a informar por escrito a FIDUCOLDEX cualquier cambio o modificación de los datos que haya suministrado referente a su composición social y Representación Legal en cualquiera de sus órganos o demás actos que sean sujetos a registro ante la Cámara de Comercio, dentro de los cinco (5) días hábiles siguientes a la ocurrencia del respectivo hecho.

PARÁGRAFO TERCERO: El reiterado incumplimiento del **CONTRATISTA**, en relación con la obligación de actualización de información contenida en la presente Cláusula, podrá a juicio de la FIDUCIARIA, dar lugar a la terminación anticipada y unilateral del presente Contrato, sin lugar al pago de indemnización o sanción alguna en favor del **CONTRATISTA**.

VIGÉSIMA SÉPTIMA. INHABILIDADES, INCOMPATIBILIDADES Y CONFLICTOS DE INTERÉS. EL CONTRATISTA declara bajo la gravedad del juramento, que conoce y acepta el Código de Buen Gobierno Corporativo de FIDUCOLDEX como vocera del patrimonio autónomo **FONTUR**, que se encuentra publicado en la página, así mismo declara no estar incurso en ninguna causal de inhabilidad e incompatibilidad para contratar con FIDUCOLDEX - **FONTUR**, ni en ninguna hipótesis de conflicto ni de coexistencia de interés.

VIGÉSIMA OCTAVA. CLÁUSULA DE INDEMNIDAD. EL CONTRATISTA mantendrá indemne al **FONTUR** de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de las de los subcontratistas o de la de sus dependientes, de conformidad con la normatividad vigente.

VIGÉSIMA NOVENA. PROHIBICIÓN DE SUBCONTRATACIÓN. EL CONTRATISTA no podrá subcontratar la totalidad del objeto del Contrato. No obstante, podrá subcontratar parcialmente actividades del alcance del objeto contractual. Esta actuación deberá ser informada a la supervisión del Contrato. En todo caso, **EL CONTRATISTA** responderá por la ejecución del cien por ciento (100%) del cumplimiento del objeto del Contrato y de las actividades derivadas del mismo en los términos y condiciones del Contrato, en consecuencia, el cumplimiento del Contrato no

quedará condicionado al cumplimiento de los Contratos u obligaciones convenidas entre **EL CONTRATISTA** y su subcontratista.

TRIGÉSIMA. INEXISTENCIA DE RELACIÓN LABORAL. Entre **EL CONTRATISTA**, las personas que este emplee para la ejecución del Contrato, y **FONTUR**, no existe relación laboral de carácter permanente o continuada, ni subordinación, ni dependencia alguna, llámese esta técnica, personal, económica o simplemente jurídica y así lo declaran y estipulan las partes.

TRIGÉSIMA PRIMERA. LIQUIDACIÓN. De conformidad a lo establecido en el numeral 7.1, Capítulo VI *"Etapa Postcontractual"* del Manual de Contratación de **FONTUR**, el presente Contrato se liquidará en un plazo que no supere los seis (06) meses contados a partir de la expiración del plazo contractual, la liquidación se fundamentará en el informe final de supervisión.

TRIGÉSIMA SEGUNDA. DOMICILIO CONTRACTUAL Y LUGAR DE EJECUCIÓN. Las partes convienen en señalar como domicilio contractual y como lugar de ejecución la ciudad de Bogotá.

TRIGÉSIMA TERCERA. PERFECCIONAMIENTO Y EJECUCIÓN DEL CONTRATO. El Contrato requiere para su perfeccionamiento de la firma de las partes, se entenderá aceptado por las partes con su firma electrónica a través de la plataforma SECOP II y para su ejecución de la aprobación de las garantías a través de la misma plataforma.

TRIGÉSIMA CUARTA. LEGISLACIÓN APLICABLE. El Contrato se rige por las normas civiles y comerciales colombianas.

TRIGÉSIMA QUINTA. MODIFICACIONES. Cualquier modificación al Contrato deberá constar en documento escrito firmado por las partes contratantes, y presentadas a través del Supervisor del Contrato con mínimo quince (15) días de anticipación.

TRIGÉSIMA SEXTA. FUERZA MAYOR Y CASO FORTUITO. En caso de que se presenten eventos que configuren fuerza mayor o caso fortuito, al tenor de las disposiciones legales colombianas, las partes podrán suspender o terminar el Contrato sin que haya lugar a la imposición de la cláusula penal.

TRIGÉSIMA SÉPTIMA. MÉRITO EJECUTIVO. El Contrato presta mérito ejecutivo por ser una obligación clara, expresa y exigible para las partes.

TRIGÉSIMA OCTAVA. DOCUMENTOS DEL CONTRATO. Se consideran documentos del Contrato y hacen parte integral del mismo los siguientes:

a) Solicitud de contratación y soportes.
b) Invitación Abierta FNTIA–016-2026 y anexos.
c) Documentos de EL CONTRATISTA.

TRIGÉSIMA NOVENA. COMUNICACIONES. Cualquier notificación o comunicación que deban remitirse las partes será dirigida a las siguientes direcciones:

- **FONTUR:** Calle 28 # 13 A 24 Edificio Museo Parque Central Piso 6 Torre B, Bogotá D.C., Colombia, Teléfono 601 7470909, Correo electrónico: contactenos@fontur.com.co

- **EL CONTRATISTA:** XXXXXXXXXXXXXXX; Teléfono XXXXXXXXXXX; correo electrónico: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Cualquier cambio de dirección para efecto de notificaciones deberá ser comunicada por las partes en forma escrita.

El presente documento se anexa y hace parte integral del Contrato Electrónico y el mismo se entiende leído y aceptado por las partes con su firma electrónica del Contrato **FNTCE-XXXX-XXXX** a través de la plataforma SECOP II.