Bogotá, D.C., junio de 2026

ANEXO TÉCNICO

ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR

Características Técnicas

Tabla 1 – Ficha técncia General

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

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Fichas técnicas Específicas

Tabla 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 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.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
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 de la Entidad 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 de la Entidad, 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. • 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 de la entidad.
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.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
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.
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.

Especificaciones técnicas del SIEM - Plataforma correlacionador de eventos
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. • 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
La entidad 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

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Tabla 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 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 de la Entidad • 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 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

Especificaciones técnicas - Protección del Entorno de Trabajo
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) • 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

Especificaciones técnicas - Protección del Entorno de Trabajo
• 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.

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Tabla 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
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

Especificaciones Técnicas - Logs y reportes
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).
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

Especificaciones Técnicas - Logs y reportes
Los siguientes hacen referencia a los Reportes asociados a la actual Arquitectura Fortinet de le Entidad. 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: • 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

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Tabla 5 – XDR - Extended Detection and Response

Especificaciones Técnicas - XDR - Extended Detection and Response
Generalidades • La Entidad requiere del licenciamiento de la solución xDR/EDR para 500 dispositivos. • La solución de xDR/EDR debe proporcionar a la Entidad 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.

Especificaciones Técnicas - XDR - Extended Detection and Response
• 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:
 	
• 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 en la entidad. 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.

Especificaciones Técnicas - XDR - Extended Detection and Response
• Proceso inyectado. • Hilo inyectado. • Suma de comprobación no válida. • Ejecución no válida. • Puntero no válido. • 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 de la entidad, 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. • 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:

Especificaciones Técnicas - XDR - Extended Detection and Response
• Next Generation Firewall de la Entidad • 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 de la entidad. • Hibrida: En Nube y On-premise. • AirGapped o Sistemas Cerrados.

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Tabla 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. • 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.

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

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</td></tr>
<tr><td>Transferencia de Conocimiento</td><td>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.</td></tr>
</table>

	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, indicando al menos marcas, modelos y referencias de los bienes ofertados. 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 Autónomo.

Fuente. FICHA TÉCNICA ADQUISICIÓN DE HERRAMIENTAS TECNOLÓGICAS ESPECIALIZADAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA Y PERIMETRAL DEL P.A. FONTUR-OFICINA DE TECNOLOGÍA P.A. FONTUR. Fecha de consulta enero 21 del 2026.

Tabla 7 – PERSONAL MÍNIMO REQUERIDO PARA LA EJECUCIÓN DEL CONTRATO.

ROL	PERFIL	EXPERIENCIA	CERTIFICACIONES
Gerente de Proyecto	Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de sistemas y/o afines según área de conocimiento clasificación SNIES.	**Experiencia General** Siete (7) años de experiencia a partir de la expedición de la tarjeta profesional. **Experiencia Específica:**	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).
	Postgrado en Sistemas Gerenciales de Ingeniería o Gerencia de Proyectos o Especialista en Seguridad de la Información.	Cinco (5) años de experiencia como líder de Implementación en conocimiento y gestión de proyectos.	
	Título Pregrado (adjuntar acta de grado o diploma). **Título Posgrado** Matricula profesional vigente (Adjuntar copia digital de la tarjeta y certificado de vigencia de este documento). Certificado de antecedentes disciplinarios emitidos por el Consejo Profesional Nacional de Ingeniería – COPNIA.	**Nota1:** La experiencia general será contada a partir de la expedición de la Tarjeta Profesional, conforme certificados emitidos 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. **Nota 2:** 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.	
		Nota 3: El oferente deberá presentar todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso de adquisición. La no presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación.	

Líder de Instalación y Conectividad	Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de sistemas y/o afines según área de conocimiento clasificación SNIES. **Título Pregrado** (adjuntar acta de grado o diploma). Matrícula profesional vigente (Adjuntar copia digital de la tarjeta y certificado de vigencia de este documento). Certificado de antecedentes disciplinarios emitidos por el Consejo Profesional Nacional de Ingeniería – COPNIA	**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. **Nota1:** La experiencia general será contada a partir de la expedición de la Tarjeta Profesional, conforme certificados emitidos 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. **Nota 2:** 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. **Nota 3:** El oferente deberá presentar todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso de adquisición. La no presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación.	El Ingeniero líder de instalación y conectividad deberá contar con al menos tres (3) certificaciones vigentes del fabricante de la solución ofertada, relacionadas con instalación, conectividad, seguridad de red, operación de seguridad, implementación o soporte técnico de las herramientas objeto del contrato. Dentro de las cuales se pueden presentar: A. Fortinet B. Certified Professional C. Secure Networking. D. Fortinet Certified Professional Security Operations. Las certificaciones deberán corresponder a las indicadas por el fabricante en los siguientes portales: https://www.fortinet.com/lat/training-certification https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortinet-expands-nse-certification-program-to-address-evolving-cybersecurity-skillset-needs

ROL	PERFIL	EXPERIENCIA	CERTIFICACIONES
Líder de Ingeniería - Implementador	Áreas de Ingeniería Electrónica, Telemática o Telecomunicaciones y/o Ingeniería de sistemas y/o afines según área de conocimiento clasificación SNIES. **Título Pregrado** (adjuntar acta de grado o diploma). **Título Posgrado.** Matrícula profesional vigente (Adjuntar copia digital de la tarjeta y certificado de vigencia de este documento). Certificado de antecedentes disciplinarios emitidos por el consejo profesional nacional de ingeniería – COPNIA.	**Experiencia General:** Diez (10) años de experiencia a partir de la expedición de la tarjeta profesional. **Experiencia Específica:** Siete (7) años de experiencia como líder de Implementación en conocimiento y gestión de proyectos. **Nota1:** La Experiencia general será contada a partir de la expedición de la Tarjeta Profesional, conforme certificados emitidos 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. **Nota 2:** 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. **Nota 3:** El oferente deberá presentar todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso de adquisición. La NO presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación.	**Posgrado y/o Maestrías en:** Seguridad de las tecnologías de la información y/o de las comunicaciones o administración de riesgos informáticos o seguridad informática. 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 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.