

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016

Ficha Técnica


1. PRESTAR LOS SERVICIOS DE ADMINISTRACIÓN, ACTUALIZACIÓN, SOPORTE TÉCNICO ESPECIALIZADO, MANTENIMIENTO PREVENTIVO Y CORRECTIVO INCLUYENDO REPUESTOS PARA LOS SISTEMAS DE CIBERSEGURIDAD DEL CONCEJO DE BOGOTÁ D.C.	
Denominación del Bien:	Prestar los servicios de renovación del licenciamiento, soporte de fábrica, mantenimiento preventivo y correctivo incluido repuestos para los equipos de ciberseguridad del Concejo de Bogotá D.C.
Denominación Técnica:	Servicio de soporte, administración, actualización, renovación de licenciamiento, mantenimiento preventivo y correctivo para los equipos de ciberseguridad y monitoreo informático a la red de datos y servidores del Concejo de Bogotá D.C.
Objeto:	Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.
1.1 Justificación: <p>El Proceso de Tecnologías de la Información del Concejo de Bogotá tiene a su cargo la gestión, administración y mantenimiento de los recursos tecnológicos, plataformas, sistemas y software con los que cuenta la Corporación, en los que se encuentran entre otros para Seguridad Informática y Ciberseguridad; dos (2) Firewall de nueva generación NGFW – FortiGate 1000D, dos (2) Firewall de aplicaciones Web (FortiWeb) en cluster para protección de aplicaciones y servicios web, un (1) FortiAnalyzer para almacenamiento de los logs, ejecución de consultas y generación de reportes, una (1) plataforma SIEM del fabricante FORTINET Virtual Appliance (FortiSIEM) para monitoreo y correlación de eventos, una (1) solución de Control de Acceso a la red (FortiNAC) desplegada en máquinas virtuales para control de acceso a red de datos, los cuales hacen parte del sistema de seguridad y monitoreo informático actual del Concejo de Bogotá D.C., que permiten el control, registro y monitoreo constante de eventos que se presentan en varios componentes de la infraestructura tecnológica de la Corporación. Esto es de relevante importancia para tomar acciones inmediatas ante cualquier eventualidad, así como proteger uno de sus activos más valiosos, la información.</p> <p>La infraestructura de seguridad informática y ciberseguridad proporciona los mecanismos de protección y respuesta ante incidentes informáticos como intentos de captura de información, denegación de servicios, suplantación a la página web de la Corporación, acceso no autorizado a la red, entre otros. Para su buen y normal funcionamiento, los equipos relacionados en la presente ficha requieren contar con actualizaciones generales, de firmware, suscripción a los servicios de soporte avanzado 24x7 y dar la continuidad a los servicios con que cuentan actualmente las plataformas. Así mismo, se requiere contar con los servicios profesionales para soporte preventivo y correctivo a las plataformas, atención de incidentes sobre las plataformas renovadas, apoyo en la gestión y configuraciones sobre las mismas por personal especializado, consultas a través de llamadas telefónicas y correo electrónico.</p> <p>El equipo FortiAnalyzer actualmente en operación tiene fin de su vida útil (End of Life – EOL) el 14 de julio de 2026, de acuerdo con las políticas del fabricante. Esta condición implica que el dispositivo no contará con soporte técnico oficial, actualizaciones de firmware, ni parches de seguridad luego de esta fecha, lo cual representa un riesgo significativo para la continuidad operativa y la seguridad de la infraestructura tecnológica del Concejo de Bogotá, D.C.</p> <p>Por lo anterior, se hace necesario realizar la sustitución del equipo por una versión más actualizada, que garantice soporte vigente, mayor capacidad de procesamiento, mejores funcionalidades de</p>	

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>seguridad Fortinet en el Concejo de Bogotá, D.C., (los requerimientos técnicos se listan en el numeral 3 de este documento).</p> <p>** Teniendo en cuenta que, el licenciamiento de Fortimail Cloud expiró, se requiere actualizar la solución para mantener el aseguramiento informático del correo electrónico en nube con que cuenta el Concejo de Bogotá D.C., (los requerimientos técnicos se listan en el numeral 4 de este documento).</p> <p>Así mismo, se requiere continuidad de la prestación del servicio de monitoreo SOC (Security Operation Center) con alcance de detección, respuesta y remediación por el termino de vigencia del contrato en horario 7x24.</p> <p>El contratista deberá:</p> <ul style="list-style-type: none"> • Cumplir con la política de seguridad de la información y la política de privacidad de los datos de la Corporación. • Realizar la instalación, implementación, configuración sobre los equipos y puesta en marcha del licenciamiento ofertado. • Realizar afinamiento (tunning) sobre cada uno de los equipos relacionados, consistente en revisión de las configuraciones de políticas, reglas, objetos, entre otros implementadas sobre los equipos, a fin de depurar para optimizar el consumo de recursos de acuerdo con las mejores prácticas. • Realizar endurecimiento (hardening) sobre cada uno de los equipos relacionados, consistente en revisión de las arquitecturas y configuraciones implementadas a fin de mejorar la arquitectura de seguridad informática, proponiendo las mejoras y ejecutando las actividades y configuraciones que sean necesarias para ello, de acuerdo con las recomendaciones según los hallazgos identificados por el Contratista. • Planear cada una de las actividades, validadas en conjunto con el Concejo de Bogotá D.C. • Configurar y alistar el software y firmware del hardware a la última versión estable aprobada por el fabricante, de acuerdo con diagnostico a cargo del contratista y necesidades de la Corporación. • Implementar las licencias ofertadas de acuerdo con las mejores prácticas del fabricante. • Realizar pruebas de servicio de las plataformas. • Realizar puesta en marcha de las plataformas. • Configurar y estabilizar las plataformas implementadas. • El contratista durante la ejecución del contrato presentará informes periódicos de ejecución de las actividades (implementación de licencias, mantenimientos preventivos y correctivos). <p>Será responsabilidad del contratista, la implementación de medidas de remediación de incidentes y vulnerabilidades que se deriven de</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>eventos de seguridad detectados y reportados por el Concejo de Bogotá D.C., y que sean de alcance y gobernabilidad de remediación desde las plataformas de seguridad perimetral objeto del presente contrato.</p> <p>La renovación debe incluir soporte postventa y acompañamiento por parte de un canal autorizado por el fabricante, por lo menos en uno de los niveles de membresía más alta ante fabricante. Lo cual deberá ser evidenciado por el oferente en la presentación de su propuesta, mediante la presentación de carta emitida por el fabricante donde se especifique el nivel de membresía y las plataformas ofertadas.</p> <p>La carta emitida directamente por fabricante debe estar dirigida al Concejo de Bogotá D.C., evidenciar que es distribuidor autorizado en el máximo nivel de membresía del fabricante, especificar que el oferente cuenta con al menos (2) dos especializaciones, una de las cuales deberá ser SD-WAN y la otra especialidad deberá ser relacionada con seguridad dentro de los componentes que son parte del presente proceso (Public Cloud Security, Security Operations o Operational Technology), y tener una fecha de expedición no mayor a treinta (30) días, antes de la presentación de la oferta.</p> <p>El oferente debe presentar junto con su propuesta una carta emitida directamente por fabricante donde se indique que cuenta con personal certificado de acuerdo con lo establecido en el anexo técnico, adjuntando las certificaciones vigentes y expedidas por los fabricantes de las plataformas renovadas.</p> <p>El oferente debe presentar carta firmada por el representante legal donde se indique claramente el compromiso a mantener los niveles de membresía de los fabricantes y el personal técnico certificado durante la vigencia del contrato y que en caso de cambio de personal en cinco (5) días hábiles presentará las hojas de vida y certificaciones de los fabricantes que cumplan con los requisitos técnicos establecidos en la presente ficha técnica.</p> <p>El contratista como receptor de información en virtud del contrato que se ejecute, tendrá la obligación de proteger la información que la entidad le suministre, incluyendo la confidencialidad, integridad y disponibilidad de la información.</p> <p>El contratista y su personal, excepto previo consentimiento por escrito de la Corporación, no podrán revelar en ningún momento a cualquier persona, empresa o entidad ninguna información confidencial adquirida en el curso de la prestación de los servicios; ni el proveedor ni su personal podrán publicar o dar a conocer las recomendaciones formuladas en el curso de o como resultado de este proceso.</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>Se debe realizar entrega a satisfacción a la Corporación de las licencias y servicios requeridos, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la Corporación.</p> <p>El contratista deberá realizar instalación, implementación, puesta en marcha de las renovaciones requeridas en el presente proceso y afinamiento sobre las plataformas renovadas, que incluye acompañamiento en la depuración de políticas, reglas, objetos, métodos, pools, entre otros de acuerdo con diagnóstico realizado sobre cada una de las plataformas y acompañamientos a personal de la Corporación de acuerdo con las recomendaciones realizadas a partir del diagnóstico a cargo del contratista.</p> <p>Se deberá realizar planeación de cada una de las actividades, validadas en conjunto con el Concejo de Bogotá D.C., diligenciando los formatos que sean indicados por la Corporación, sin perjuicio de los que maneje el contratista.</p> <p>En todo momento, los servicios prestados se realizarán de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura, deberá incluir pruebas de servicios de las plataformas renovadas, así como de los soportados sobre las mismas y entrega a satisfacción de la Corporación.</p> <p>Todos los servicios de soporte y mantenimientos (correctivo y preventivo) deberán ser prestados por personal certificado por los fabricantes.</p>
2.2	Soporte directo por fabricante	<p>Extender la renovación de las licencias y servicios de actualización, soporte y mantenimiento anual para los equipos relacionados en el ítem 2.1 a partir de la fecha de finalización de los contratos actuales en la modalidad 7x24 ante fabricantes.</p> <p>La renovación deberá realizarse como mínimo en las mismas condiciones de licenciamiento actual. En todo caso el proveedor deberá contemplar todas las firmas y suscripciones necesarias para que las plataformas queden totalmente licenciadas y con las características activas hasta la fecha requerida.</p> <p>El oferente debe contemplar todo el suministro de Hardware, Software, licenciamiento, servicios profesionales, cables y accesorios en general que se requieran para dar cumplimiento a la instalación, implementación y puesta en marcha de las renovaciones y mantenimiento y operación adecuada de las soluciones de seguridad relacionadas en la presente ficha técnica.</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
2.3	Reemplazo de partes	<p>El contrato de soporte deberá incluir el reemplazo de las partes necesarias para garantizar el correcto funcionamiento de los equipos objeto del contrato sin costo adicional para el Concejo de Bogotá D.C.</p> <p>Los repuestos deberán ser originales y homologados por el fabricante, y entregados e instalados en las sedes de la Corporación salvo que sea indispensable el traslado del equipo a los laboratorios del proveedor.</p> <p>Los equipos o partes que reciba el Concejo de Bogotá D.C., en reemplazo de los dañados, pasarán a ser propiedad del Concejo. El equipo o partes dañados deberán ser retirados por el contratista, previa coordinación con el personal de la Corporación.</p>
3. SOLUCIÓN DE CONTROL DE ANALÍTICA Y GESTIÓN DE LOGS		
Se deberá suministrar y actualizar la solución de análisis y gestión de registros de seguridad en appliance dedicado, la cual permitirá la recolección, almacenamiento, correlación y análisis de los registros generados por los dispositivos de seguridad y red de la entidad. Esta solución deberá integrarse con los firewalls de nueva generación actuales del Concejo de Bogotá D.C. y con los demás equipos que conforman el ecosistema de seguridad existente, para lo cual el contratista deberá garantizar que cuenta con los respectivos servicios profesionales.		
3.1	Generalidades	<ul style="list-style-type: none"> • Sistema de almacenamiento de logs y reportes con sistema operativo propietario, interfaz gráfica vía HTTPS y acceso CLI por SSH. • Capacidad de definir dominios administrativos (ADOMs) y múltiples roles de administradores para segmentar la operación. • Integración segura de dispositivos Fortinet y de terceros mediante colectores de logs; posibilidad de definir cuotas de disco por dispositivo y registrar métricas de almacenamiento y tiempo restante. • Arquitectura escalable con roles de recolector y analizador para optimizar el manejo y procesamiento de logs. • Posibilidad de asignar espacio de almacenamiento específico a cada instancia (virtual o física) y alertas cuando se alcanza un umbral. • Políticas de contraseñas robustas, autenticación multifactor y gestión de cuentas con expiración. • Visualización en tiempo real de logs y exportación en formatos CSV/JSON; generación de bitácoras de auditoría con cambios administrativos y hora. • Capacidad de replicar reportes existentes para modificarlos, exportar logs, crear filtros y personalizar gráficos y tablas. • Envío automático de logs a servidores externos (FTP/SFTP) y notificaciones de eventos por correo electrónico, SNMP o Syslog. • Dashboards personalizables que muestren tráfico, categorías de URL, amenazas y servicios, con indicadores de compromiso para usuarios finales.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Herramientas de diagnóstico de rendimiento y visualización del estado del sistema (licencias, memoria, CPU, tasa de logs por segundo). Soporte de alta disponibilidad y fail over automático para garantizar continuidad de servicio. Compatibilidad con IPv4 e IPv6 y con formatos de registro estándar como syslog, CEF y LEEF. Soporte para cifrado en reposo de la base de datos de logs y comunicaciones cifradas entre dispositivos. Políticas de retención de datos configurables por tipo de log y por dispositivo. Sincronización horaria con NTP y registro de logs con sello de tiempo preciso. Soporte para autenticación externa mediante LDAP/Active Directory o RADIUS. Integración con SNMP para envío de traps y supervisión por herramientas de monitoreo. API REST para automatizar tareas de administración y extracción de datos. Capacidad de actualización de software sin interrupción mediante proceso de *rolling upgrade*. Posibilidad de replicar datos a un sitio de respaldo o nube para contingencia y continuidad del negocio. Capacidad de etiquetar logs y datos para facilitar búsquedas posteriores. Soporte para clusters activos activos o activos pasivos con balanceo de carga.
3.2	Generación de reportes	<ul style="list-style-type: none"> Personalizar el contenido de los reportes (tablas y gráficos) y criterios de filtrado (fuentes, destinos, servicios, periodos relativos y absolutos). Programar reportes y enviarlos automáticamente a múltiples destinatarios por correo electrónico. Disponibilidad de exportación en formatos PDF, HTML, XML, CSV y envío a repositorios externos. Soporte de múltiples idiomas (español e inglés) y personalización de portada, logotipos, colores y diseño (gráficos, texto, imágenes). Plantillas integradas para normativas PCI DSS v4.0.1, NIST CSF, NIST 800 53, IEC 62443 y otras. Capacidad de clonar y modificar reportes existentes para ajustarlos a las necesidades del cliente. Reportes de utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y servicios con mayor consumo. Reportes de ataques detectados/detenidos con mayor frecuencia, por fuente y/o destino. Reportes de páginas y categorías de URL visitadas con mayor frecuencia.

 <p>CONCEJO DE BOGOTÁ, D.C.</p>	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Reportes sobre virus detectados/removidos a nivel de red, por fuente y/o destino. Reportes de actividades administrativas (ingresos de administradores, cambios de configuración). Personalización de criterios de obtención de reportes: fuentes, destinos, servicios, fechas y días de la semana. Especificación de periodos de tiempo (hoy, ayer, esta semana, semana pasada, mes actual, mes anterior) o periodos absolutos. Capacidad de calendarizar reportes con periodicidad variable (horaria, diaria, semanal, mensual). Envío automático de reportes a servidores SFTP o FTP. Inclusión de gráficos variados: barras, líneas, pastel y tablas comparativas. Reportes de rendimiento de dispositivos, top aplicaciones y usuarios con mayor ancho de banda. Reportes de reputación de IP/URL y seguridad web. Reportes de tráfico VPN (usuarios conectados, duración de sesiones). Reportes de prevención de pérdida de datos (DLP), IPS, reputación de clientes, análisis de usuario y amenazas. Reportes de uso de aplicaciones SaaS y seguridad de correo electrónico. Reportes de sandboxing, antispam e integridad de archivos. Reportes de actividad de usuarios privilegiados y contraseñas débiles. Reportes de eventos industriales/OT y cumplimiento GDPR. Capacidad de generar informes de tendencias y pronósticos a partir de datasets. Exportación de datos a plataformas de Business Intelligence para análisis adicional. Creación de bibliotecas de reportes reutilizables y compartirlas entre administradores.
3.3	Análisis forense y correlación	<ul style="list-style-type: none"> Búsqueda forense por nombre de usuario, IP, dispositivo o cualquier atributo y generación de informes de seguimiento de actividad. Módulo **Incidents & Events** con reglas de correlación y manejadores de eventos para identificar alto volumen de DNS, ataques DDoS, múltiples fallos de inicio de sesión, explotación de vulnerabilidades, etc. Capacidades de *drill down* para ir de los eventos correlacionados a los logs brutos y viceversa. Creación de reglas de correlación personalizadas mediante definiciones basadas en atributos de logs y umbrales. Correlación de eventos entre distintos dispositivos y ADOMs, permitiendo entender la secuencia de la amenaza. Visualización de la cadena de eventos en una línea temporal y establecimiento de relaciones causa efecto.

 <p>CONCEJO DE BOGOTÁ, D.C.</p>	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Definición de umbrales y condiciones para alertas automáticas y escalamiento. Búsqueda avanzada con operadores lógicos, comodines, rangos de fechas y filtros combinados. Conservación de histórico forense configurable (meses o años) para análisis a largo plazo. Etiquetado de eventos de interés para agrupar investigaciones y facilitar su seguimiento. Integración con servicios externos de inteligencia de amenazas para enriquecer la correlación. Identificación de hosts y usuarios implicados mediante correlación cruzada entre diferentes tipos de logs (tráfico, eventos, antivirus). Exportación de resultados de análisis forense a herramientas de terceros (p. ej., plataformas de SIEM externas) en formato estándar. Notificaciones a analistas mediante panel, correo o mensajería instantánea cuando se detectan correlaciones críticas. Aplicación de técnicas de análisis de comportamiento para detectar desviaciones y anomalías. Auditoría completa de las consultas forenses realizadas y de los cambios en reglas de correlación. Informes automáticos sobre correlaciones y tendencias de amenazas detectadas. Importación de listas negras, indicadores de compromiso (IoC) y reglas adicionales desde fuentes externas. Creación de dashboards específicos para análisis forense con gráficos y tablas relacionadas. Filtrado de resultados por tipo de log (tráfico, aplicación, vulnerabilidad, OT, etc.).
3.4	Características mínimas de desempeño	<ul style="list-style-type: none"> Soporte para compresión de logs y cifrado de datos en reposo. Posibilidad de replicar los logs a almacenamiento externo (NAS/SAN) o repositorios externos para archivado. Purgado automático de logs según políticas de ciclo de vida y requisitos regulatorios. Visualización del uso de disco por tipo de log y por dominio administrativo, con alertas de espacio disponible. Notificaciones cuando el almacenamiento disponible alcanza umbrales configurables. Integración con soluciones de respaldo para copias periódicas de datos. Programación de tareas de limpieza y optimización de índices fuera de horario productivo. Registro de metadatos asociados a cada log almacenado (origen, destino, tamaño, duración u otros atributos disponibles). Monitorización del rendimiento del almacenamiento y del sistema. Capacidad de procesamiento de logs hasta 200 GB por día.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Tasa sostenida de análisis de hasta 4.000 logs por segundo y hasta 6.000 logs por segundo en modo colector. Periodo de retención de logs en línea mínimo de 1 mes, configurable según políticas de almacenamiento. Capacidad de almacenamiento local de 16 TB. Interfaces de red: 4 x puertos Gigabit Ethernet RJ-45 y 2 x puertos Gigabit Ethernet SFP. Capacidad de integración con hasta 800 dispositivos o VDOMs para recepción centralizada de logs.
3.5	Administrador de dispositivos	<ul style="list-style-type: none"> Registro automático de nuevos dispositivos y validación de identidad. Categorización por tipo de dispositivo (FortiGate, FortiSwitch, FortiAP, terceros, etc.). Asignación de políticas de log y de retención por dispositivo. Configuración de cuotas de almacenamiento y control del consumo. Activación o desactivación del envío de logs por dispositivo según políticas. Asignación de etiquetas, grupos y comentarios a los dispositivos para organización. Personalización de columnas y vistas en la tabla de dispositivos. Auditoría de todos los cambios de configuración aplicados desde el administrador. Búsqueda avanzada por nombre, IP, modelo, versión de firmware o etiqueta. Visualización de los dispositivos con mayor volumen de logs y generación de gráficas. Recepción de notificaciones de desconexión o fallas de dispositivos. Delegación de la administración a sub administradores por ADOM o grupo. Gestión de certificados para dispositivos que utilicen TLS para el envío de logs. Control de listas de confianza para autorización de miembros en FortiAnalyzer Fabric. Capacidad de agrupar dispositivos por zonas geográficas o departamentos.
3.6	Security fabric	<ul style="list-style-type: none"> Compartición de indicadores de compromiso (IoC) y telemetría entre FortiGate, FortiClient, FortiAnalyzer y otros componentes del Fabric. Visualización de la topología de la malla de seguridad, incluyendo enlaces y segmentos. Correlación de eventos entre firewall, EDR, correo electrónico, switches, APs y otros dispositivos. Integración opcional con FortiAI y FortiNDR para análisis avanzado.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • Delegación de reglas de automatización a otros productos del Fabric (FortiOS Automation, FortiSOAR). • Unificación de autenticación mediante FortiAuthenticator y gestión de identidades. • Integración con telemetría de endpoints y evaluación del estado de seguridad de clientes. • Bloqueo automático de IPs maliciosas en FortiGate a partir de alertas de FortiAnalyzer. • Compatibilidad con Fabric Connectors para nubes públicas (AWS, Azure, GCP) y SaaS. • Visualización del *Security Rating* de la malla y recomendaciones de mejora. • Integración con servicios SASE como FortiSASE para extender la seguridad a usuarios remotos. • Orquestación de cambios de red mediante flujos de automatización de FortiOS. • Monitorización de la salud de cada componente del Fabric (latencia, CPU, memoria). • Reportes unificados de incidentes y amenazas a nivel de toda la malla. • Integración con soluciones de terceros mediante APIs abiertas.
3.7	Manejo de incidentes	<ul style="list-style-type: none"> • Creación automática de incidentes a partir de eventos correlacionados, clasificándolos por severidad y prioridad. • Asignación de propietarios, estados y plazos (SLA) a cada incidente. • Asociación de múltiples eventos o alarmas a un mismo incidente para un análisis consolidado. • Adjuntar archivos, capturas de pantalla o evidencias al expediente del incidente. • Clasificar incidentes por categoría (malware, phishing, violación de políticas, etc.). • Configurar flujos de trabajo de aprobación y escalamiento automático según criticidad. • Registrar fecha de apertura, cierre y tiempos de respuesta para evaluar el cumplimiento de SLA. • Integración con sistemas de ticketing (Jira, ServiceDesk Plus, Zendesk, Freshservice) para creación, actualización y cierre de tickets. • Permitir comentarios, notas y comunicaciones entre los miembros del equipo dentro del incidente. • Posibilidad de reabrir incidentes cerrados cuando se detectan eventos relacionados. • Filtrado y búsqueda avanzada de incidentes por estado, propietario, severidad o categoría. • Generación de informes históricos de incidentes para análisis de tendencias y desempeño del SOC.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Plantillas de respuesta rápida con acciones predefinidas por tipo de incidente. Exportación de incidentes a formatos estándar para auditorías y revisiones externas. Integración con notificaciones push, SMS o plataformas de mensajería para alertas inmediatas. Análisis de causa raíz y registro de lecciones aprendidas para mejorar procesos. Soporte para clasificación de incidentes según MITRE ATT&CK.
3.8	Inteligencia artificial y analítica	<ul style="list-style-type: none"> Análisis de amenazas basado en modelos de aprendizaje automático y detección de anomalías. Clasificación automática de logs según tipo y gravedad de evento. Predicción de tendencias de ataques y proyección de crecimiento de amenazas. Recomendaciones automáticas de remediación basadas en patrones históricos. Priorización de alertas en función del riesgo y contexto de la organización. Generación automática de resúmenes de incidentes para rápida comprensión. Escalamiento automático de alertas según políticas definidas. Interacción con asistentes de IA para realizar investigaciones conversacionales. Entrenamiento continuo de modelos con datos locales para mejorar precisión. Integración con servicios de IA de FortiGuard Labs para clasificación de amenazas. Correlación de datos con feeds de inteligencia global y local. Creación de modelos personalizados de detección para casos específicos del cliente. Optimización de políticas de seguridad mediante análisis predictivo. Ajuste dinámico de algoritmos según retroalimentación del operador. Presentación de puntuaciones de riesgo por usuario, dispositivo y aplicación. Identificación automática de campañas de phishing y malware dirigidas. Segmentación de datos para proteger la privacidad y cumplir regulaciones. Análisis de sentimiento de los mensajes y correos para detectar posibles fraudes. Comparación automática de patrones locales con la base de conocimiento global. Uso de IA generativa para sintetizar respuestas y recomendaciones.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> El asistente de IA generativa (FortiAI) debe estar integrado en FortiAnalyzer y aprovechar los registros unificados, alertas y telemetría para monitorear y analizar alertas, realizando triage y respuestas a incidentes basados en inteligencia contextual. Debe permitir consultas de lenguaje natural y comandos de voz con menús intuitivos para generar consultas complejas sobre la base de datos de eventos y crear informes sin necesidad de escribir código. El asistente debe proporcionar inteligencia contextual y sugerencias de respuesta a incidentes, generando gráficos y tablas basados en los registros y alertas relevantes para mejorar la visualización y análisis. Debe permitir la priorización de tareas y vulnerabilidades, pudiendo identificar las vulnerabilidades críticas y los activos de mayor riesgo según el contexto de la organización. El asistente debe estar accesible desde cualquier pestaña de la interfaz de FortiAnalyzer, soportar mínimo 5 idiomas escritos y hablados y ofrecer funciones de voice-to-text, incluidos español e inglés. La licencia de FortiAI debe incluir un contingente mensual de tokens de LLM compartido entre los usuarios; el consumo de tokens debe basarse en el tamaño del prompt y la respuesta generada y mostrarse en la interfaz. Debe ofrecer visualización del uso de tokens en la interfaz de FortiAI e incluir mecanismos para adquirir paquetes adicionales cuando se alcance el límite mensual. Debe limitar el uso del asistente a un máximo de tres administradores locales por dispositivo, con capacidad de habilitar o deshabilitar FortiAI a nivel de usuario mediante GUI o CLI. Incluir buenas prácticas para optimizar el uso de tokens, tales como utilizar prompts concisos, especificar periodos y dispositivos concretos, referirse a datasets existentes y reiniciar sesiones después de 10 conversaciones. El asistente debe integrarse con playbooks de automatización para ejecutar acciones recomendadas automáticamente en entornos de SOAR, manteniendo la privacidad de los datos y garantizando que la información no se exponga a servicios externos.
3.9	Reportes predefinidos	<ul style="list-style-type: none"> Reporte de rendimiento de dispositivos: CPU, memoria, disco, tasa de logs. Reporte de top aplicaciones y servicios. Reporte de consumo de ancho de banda por usuario y por hora. Reporte de amenazas bloqueadas por el sistema de prevención de intrusos (IPS). Reporte de reputación de clientes y evaluación de riesgos. Reporte de seguridad de correo electrónico (spam, phishing, malware). Reporte de filtrado web y categorías visitadas. Reporte de seguridad de endpoints y estado de las actualizaciones.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • Reporte de uso de VPN y conexiones remotas. • Reporte de políticas de prevención de pérdida de datos (DLP). • Reporte de eventos de sandboxing y análisis dinámico de archivos. • Reporte de antispam y protección de correo electrónico. • Reporte de integridad de archivos y cambios sospechosos. • Reporte de detecciones de IDS y correlación de ataques. • Reporte de contraseñas débiles y credenciales comprometidas. • Reporte de utilización de aplicaciones SaaS y Shadow IT. • Reporte de eventos de tecnologías operativas (OT/ICS). • Reporte de cumplimiento de normativas locales e internacionales. • Reporte de usuarios privilegiados y actividades de administración. • Reporte de tráfico hacia dominios de alta reputación y dominios sospechosos. • Reporte de análisis de comportamiento de usuarios y entidades. • Reporte de amenazas de día cero identificadas por inteligencia global. • Reporte de incidentes cerrados, en curso y pendientes.
3.10	Custom log parsers	<ul style="list-style-type: none"> • Importación de parsers personalizados en formato JSON y creación a partir de expresiones regulares. • Interfaz gráfica para importar, exportar y habilitar/deshabilitar parsers. • Edición y copia de parsers existentes para crear nuevas variantes. • Documentación de la estructura y parámetros de cada parser. • Gestión de versiones y control de cambios de parsers para revertir a versiones anteriores. • Asignación automática de parsers a dispositivos en función de patrones de log. • Etiquetado y clasificación de parsers por tipo de dispositivo o aplicación. • Integración con FortiGuard para descargar mensualmente nuevos parsers de terceros. • Soporte para logs en formato JSON, CEF, LEEF y syslog tradicional. • Compatibilidad con parsers de logs de aplicaciones web y servicios en la nube. • Soporte para importar parsers a granel desde paquetes.
3.11	Security operations	<ul style="list-style-type: none"> • Definir roles y responsabilidades del SOC y asignarlos en el sistema. • Integrarse con SIEM de terceros y compartir información en tiempo real. • Adherirse a marcos de referencia como NIST 800 53, ISO 27001 y MITRE ATT&CK. • Implementar programas de gestión continua de la exposición a amenazas (CTEM). • Integrar y compartir inteligencia de amenazas con fuentes externas (feed de IPs, dominios, etc.).

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • Automatizar procesos de investigación y clasificación de incidentes. • Proporcionar monitoreo 24x7 de la red, sistemas y aplicaciones. • Integrarse con sistemas de notificación y mensajería corporativa para alertas. • Coordinar acciones con equipos de redes, infraestructuras y desarrollo. • Integrarse con soluciones EDR/XDR y Endpoint Protection para correlación ampliada. • Facilitar la auditoría de seguridad y cumplimiento con registros detallados. • Proporcionar flujos de trabajo para la creación, validación y cierre de incidentes. • Soportar la integración con plataformas de gestión de vulnerabilidades. • Habilitar orquestación de respuesta entre múltiples herramientas de seguridad. • Permitir la creación de playbooks de investigación y respuesta a medida. • Facilitar la colaboración entre equipos de seguridad mediante tableros compartidos. • Automatizar informes de auditoría y cumplimiento periódicos. • Permitir la integración con herramientas de gestión de configuración y activos. • Cumplir con requisitos locales de protección de datos y privacidad.
4. SOLUCIÓN DE SEGURIDAD PARA CORREO EN NUBE		
Se deberá suministrar, instalar, configurar e implementar una solución de seguridad de protección de correo electrónico como servicio en la nube, en la modalidad de Software como Servicio (SaaS), para el servicio de correo electrónico en nube del Concejo de Bogotá D.C. para 1200 buzones.		
4.1	Implementación	La solución debe contar con un modelo de despliegue y aprovisionamiento en la nube basado en integraciones vía API que permita su implementación ágil y sin requerir modificaciones en la infraestructura de correo electrónico permitiendo la activación transparente para los usuarios finales.
4.2	Licenciamiento	Para 1200 buzones de correo, necesario para el funcionamiento de la solución con todas las características y servicios requeridos en la presente ficha técnica por un (1) año.
4.3	Funcionalidades	<ul style="list-style-type: none"> • 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 1200 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.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> 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 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 asignar 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 la 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 dé su veredicto.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • La solución debe enviar informes y resúmenes de acciones a los usuarios. • 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 para descubrir la suplantación de nombres de visualización y la suplantación de VIP. • La solución debe proteger contra ataques de día cero vía IA al inspeccionar datos a nivel de CPU. • La solución debe detectar ATO - Account Takeover (Apropiación de Cuenta) 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 debe 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.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • 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. • 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 auditoría. • 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 implementación para los usuarios a través de una invitación por correo electrónico. • 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 fuga de datos accidental o intencional interna o externa.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> 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.). 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. 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 vigencia del contrato.
5. SERVICIOS PROFESIONALES		
5.1	Niveles de servicio	<p>El contratista deberá garantizar soporte y garantía local para las plataformas renovadas en sitio, en un esquema de 7x24 [siete (7) días de la semana, veinticuatro (24) horas al día], sin limitación de tickets o incidentes a atender, ni costos adicionales para la corporación y con tiempos de identificación de fallas y restablecimiento de servicios según prioridad, de acuerdo con lo siguiente:</p> <p>PRIORIDAD 1: Las plataformas renovadas o la operación de la red o los servicios de la Corporación, administrados y configurados en las mismas se ven afectados y hay un impacto grave en la operación de la Corporación.</p> <ul style="list-style-type: none"> Tiempo estimado de identificación de falla: dos (2) horas. Tiempo de restablecimiento de servicio: ocho (8) horas, ya sea de forma remota o mediante atención en sitio desde el reporte de la falla.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>PRIORIDAD 2: Las plataformas renovadas o la operación de la red o los servicios la Corporación, administrados y configurados en las mismas, presentan un desempeño inaceptable que afectan negativamente la operación de la Corporación.</p> <ul style="list-style-type: none"> • Tiempo estimado de identificación de falla: cuatro (4) horas. • Tiempo de restablecimiento de servicio: doce (12) horas, ya sea de forma remota o mediante atención en sitio desde el reporte de la falla. <p>PRIORIDAD 3: Se requiere apoyo en la configuración y gestión de políticas sobre las plataformas para habilitar funcionalidades o servicios de TI en la Corporación:</p> <ul style="list-style-type: none"> • Tiempo estimado para dar respuesta o ampliar información: doce (12) horas. • Tiempo para ejecución de actividades o habilitación del servicio: Cuarenta y ocho (48) horas, ya sea de forma remota o mediante atención en sitio desde el reporte de la falla. <p>PRIORIDAD 4: Se requiere información o asistencia en relación a capacidades, configuraciones, productos o servicios. Hay poco o nulo impacto en las operaciones de la Corporación.</p> <ul style="list-style-type: none"> • Tiempo estimado para dar respuesta: Un (1) día hábil. • Tiempo estimado para establecer plan de trabajo en caso de requerirse: Cuatro (4) días hábiles. <p>El contratista deberá tener un mecanismo de escalamiento dentro de la organización para reportar incidentes en caso necesario.</p> <p>La metodología de escalamiento de soporte a usar es la siguiente:</p> <p>Nivel 1: Soporte Técnico del proveedor (canal). Nivel 2: Soporte Técnico Especializado (canal). Nivel 3: Soporte Técnico Fabricante.</p> <p>Contactos de soporte técnico: La entidad en conjunto con el proveedor, deberá identificar el número correspondiente de contactos y se</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>constituirán los canales autorizados para acceder a los servicios de soporte técnico.</p> <p>Se entiende el caso como atendido, cuando se han cumplido los siguientes requisitos:</p> <ul style="list-style-type: none"> • Se cuenta con un número de ticket o servicio. • Se ha realizado la asignación del caso a un agente o analista por parte del contratista. • Se ha establecido contacto por parte del contratista con la Corporación. • Se ha realizado diagnóstico inicial por parte del agente o analista del contratista sobre el incidente o solicitud realizada por la Corporación. • Se ha retroalimentado por correo o en su defecto telefónicamente al personal de Sistemas del Concejo de Bogotá sobre el incidente o requerimiento de servicio realizado. <p>Los mensajes automáticos o el escalamiento del caso al interior de la empresa del contratista NO se entenderán como atención del mismo.</p> <p>Sesiones remotas con fabricante y atención en sitio (en caso de requerirse) por parte del oferente en horario hábil y no hábil. Todo respecto a las plataformas objeto del presente proceso.</p> <p>El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramienta de trabajos, refrigerios, entre otros) requerida para que el personal asignado pueda cumplir sus funciones.</p> <p>Este ítem, así como los tiempos de respuesta y prioridades especificadas aplican tanto para los mantenimientos correctivos como para las solicitudes de soporte y apoyo en la gestión de las plataformas, configuraciones de políticas, objetos, pools, módulos, interfaces para la habilitación de servicios.</p>
5.2	Soporte	<p>Por el término de cobertura del licenciamiento, el contratista deberá contar con un centro de contacto o call center para la recepción de casos de servicio, las veinticuatro (24) horas del día, los siete (7) días de la semana, hasta la fecha de finalización del licenciamiento renovado.</p> <p>El soporte debe incluir atención de incidentes y requerimientos de servicio sobre las plataformas licenciadas, consultas técnicas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil, para el apoyo, gestión y realización de configuraciones que sean requeridas por la Corporación sobre los equipos relacionados en el presente proceso, incluidas configuración, administración de políticas, pools, objetos, vpns, bases de datos, usuarios, habilitación de módulos y servicios de las</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>plataformas, para la habilitación de funcionalidades o servicios de TI que defina la Corporación, entre otros.</p> <p>El contratista deberá tener un mecanismo de notificaciones vía correo electrónico o vía telefónica al momento de la apertura y para hacer seguimiento y cierre de los casos.</p> <p>El contratista deberá ofrecer atención en sitio o remota, las 24 horas del día, los 7 días de la semana para atención de los casos, según se requiera para solucionar lo más pronto posible y de acuerdo con lo indicado en los niveles de servicio.</p> <p>Se deberá realizar cuantas veces la entidad lo requiera en modalidad 7x24, de conformidad con lo indicado en los niveles de servicio y deberá prestarse en las instalaciones en donde se encuentren instalados los equipos, siempre y cuando la solución del caso reportado no se pueda realizar de forma remota.</p> <p>El soporte debe brindarse en forma proactiva y preventiva con el fin de evitar la interrupción al máximo del servicio, garantizando la operación correcta y permanente de las plataformas.</p> <p>El alcance del soporte es sobre la gestión de las plataformas y las configuraciones de políticas de las mismas, de acuerdo con las solicitudes realizadas por la Corporación según los casos y requerimientos que involucren los equipos relacionados en el ítem 2.1.</p> <p>Al prestar cada servicio de soporte se deberá:</p> <ul style="list-style-type: none"> • Contar con un numero de caso o ticket de servicio único que permita realizar el seguimiento correspondiente al mismo. • Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte, configuración, requerimiento, incidente y/o mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. • Consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración de los equipos o políticas. • Se debe realizar pruebas/muestras de las plataformas donde se evidencie la correcta configuración de la plataforma ofertadas después de cada implementación, prestación de servicio o ajuste que haya sido requerido por la Corporación o las necesarias para su correcto funcionamiento. <p>Estas mismas condiciones para prestación de servicios de soporte aplican para los mantenimientos correctivos y preventivos.</p>
5.3	Matriz de escalamiento	El proveedor deberá remitir la matriz de escalamiento a la Corporación, clasificando el nivel de escalamiento según el tipo y nivel del evento acorde con los Niveles de Servicio.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
5.4	Bolsa de horas	<p>El contratista deberá poner a disposición del Concejo de Bogotá D.C., una bolsa de veinte (20) horas de especialista en las plataformas Fortinet renovadas, con el fin de realizar actividades de apoyo a la Oficina de Tecnología ante cambios que sean requeridos relacionados con ajustes, rediseño, cambios de configuración en la infraestructura tecnológica de seguridad informática de los productos Fortinet renovados con que cuenta el Concejo de Bogotá D.C., y que puedan generar un impacto a la operación de la Corporación.</p> <p>Para la ejecución de la bolsa de horas se contará con el periodo total de la renovación del licenciamiento.</p>
5.5	Garantía	<p>En sitio, por el término de cobertura del licenciamiento, para la totalidad de las licencias y suscripción a los servicios contratados sobre los equipos relacionados en el presente proceso, contado a partir de la fecha de contratación.</p> <p>Durante este periodo se debe garantizar la calidad del correcto funcionamiento de los equipos en el desarrollo del cumplimiento del objeto del contrato.</p>
6. MANTENIMIENTO CORRECTIVO		
6.1	Servicio de mantenimiento correctivo	<p>Por el término de cobertura del licenciamiento, tendrá como objetivo, después de una falla o problema, la recuperación de las plataformas para que operen satisfactoriamente. Deberá cubrir el diagnostico, la formulación de alternativas de solución, la implementación de la solución seleccionada, realización de pruebas y entrega al Concejo de Bogotá D.C. la solución documentada y las recomendaciones a las que diera lugar la solución realizada.</p> <p>El proveedor atenderá los requerimientos de mantenimiento correctivo de las plataformas y los equipos reportados en sitio y efectuará la asistencia técnica ante la presencia de fallas en la modalidad 24x7, cuantas veces sea requerido por la Corporación, de conformidad con los tiempos de respuesta señalados en los niveles de servicio, siempre y cuando la solución del problema reportado no se pueda lograr mediante conexión o asistencia remota.</p> <p>En caso de ser necesario retirar los equipos de las instalaciones de la Corporación por efectos de garantía, el contratista deberá realizar reemplazo temporal de la solución en máximo veinticuatro (24) horas contadas a partir de la identificación de cambio o reemplazo, así; dieciséis (16) horas para suministro y ocho (8) horas para configuración, instalación y puesta en marcha. La plataforma que será de propiedad del oferente, deberá ser de misma referencia con iguales o superiores características y se deberá realizar el reemplazo definitivo en máximo veinte (20) días hábiles.</p>
7. MANTENIMIENTO PREVENTIVO		

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
7.1	Servicio de mantenimiento preventivo	<p>Durante la vigencia 2026 se efectuará un (1) mantenimiento preventivo de forma remota o presencial en las instalaciones de la Corporación según se requiera, para todas y cada una de las plataformas renovadas. Se realizarán garantizando la integración con los firewalls de nueva generación actuales de la entidad con el fin de que se mantenga el esquema de Security Fabric, para lo cual el contratista deberá garantizar que cuenta con los respectivos servicios profesionales.</p> <p>El alcance debe cubrir las actualizaciones menores (updates), mayores (upgrades) y prestar el apoyo para su instalación o configuración.</p> <ul style="list-style-type: none"> • El mantenimiento preventivo comprende todas aquellas actividades proactivas reactivas que permiten el correcto funcionamiento de la infraestructura. • Realizar revisión y diagnóstico de los equipos objeto del contrato, analizando cada uno de los componentes del mismo para determinar necesidades de: actualización, suministro y/o cambio de partes, reconfiguraciones y actualización de firmware. • Se realizará la visita durante la vigencia de la garantía para el mantenimiento preventivo de los equipos. Esta visita deberá coordinarse con la supervisión del contrato o a quien delegue y deberá tener en cuenta como mínimo los siguientes aspectos: <ul style="list-style-type: none"> - Se acordará con la Corporación un plan de mantenimiento para la infraestructura objeto de este contrato, el cual se aplicará durante la vigencia 2026, para lo cual se deberá suministrar y concertar con la Corporación un cronograma de actividades y fechas tentativas para su ejecución, durante los diez (10) primeros días hábiles posteriores a la suscripción del acta de inicio. - Previo a cada mantenimiento preventivo, el proveedor deberá presentar un plan de mantenimiento que incluya entre otros; minutograma de las actividades a realizar, riesgos, rollback y responsables para realizar dicho mantenimiento. - Se deberá contar con el personal calificado por el fabricante, para realizar las labores. - Se deberá realizar limpieza externa de los elementos objeto del contrato. - Revisión de la configuración y estabilidad del software del sistema. - Corrección de errores del sistema (software y hardware). - Suministro e instalación de los componentes en mal estado o en deterioro para su normal funcionamiento. - Suministrar todos los elementos necesarios para el servicio de mantenimiento preventivo de los equipos objeto del contrato. Los elementos que se vayan a utilizar deben ser de primera calidad. - Realizar todas las actividades necesarias para garantizar el buen funcionamiento de los equipos objeto del contrato y los

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>elementos que lo componen (incluye Hardening y remediación de vulnerabilidades de acuerdo con los reportes generados).</p> <ul style="list-style-type: none"> - Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma. - Configurar, revisar y afinar los reportes / logs de las plataformas. - Una vez realizado el servicio de mantenimiento preventivo, el proveedor debe entregar probado a satisfacción y en funcionamiento los equipos intervenidos. - Presentar un informe al Concejo de Bogotá para conocer el estado de los equipos intervenidos después de efectuado el servicio de mantenimiento preventivo. - En caso de daño en algún componente electrónico y/o mecánico ocasionado por uno de sus técnicos, el contratista asumirá sin costo para el contratante, el valor de la reparación con el respectivo cambio de pieza o componente dañado y esta debe ser remplazada en menos de veinticuatro (24) horas. <p>En todo caso se velará por mantener actualizados los niveles de Firmware de los componentes ofertados y renovados de acuerdo con las últimas versiones recomendadas y estables liberadas por los fabricantes.</p> <p>Al finalizar cada visita correctiva y/o preventiva el contratista deberá:</p> <ul style="list-style-type: none"> - Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. <p>El contratista deberá consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.</p>
8. SERVICIO DE MONITOREO SOC		
Prestación del servicio de SOC (Security Operation Center) con alcance de detección, respuesta y remediación por el término de seis (6) meses, en horario 7x24. Los activos a monitorear serán los que se encuentren licenciados en la herramienta SIEM del Concejo de Bogotá D.C. (50 activos y 25 agentes avanzados FIM), así mismo, para la respuesta y remediación de incidentes el contratista realizará la gestión, operación y administración de las herramientas de seguridad informática con que cuente el Concejo de Bogotá D.C., incluida la operación y administración de solución de gestión de vulnerabilidades continua. El contratista deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma del Concejo de Bogotá D.C., de tal forma que todo el know how y parametrizaciones queden para la Corporación, en ningún caso la información de logs saldrá del Concejo.		
8.1	Integraciones y operación	<ul style="list-style-type: none"> • El contratista realizará la integración y monitoreo de los dispositivos y activos que conforman la infraestructura tecnológica del Concejo de Bogotá D.C.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> El centro de operación del contratista debe garantizar condiciones de seguridad mínimas en aspectos de acceso al espacio físico y acceso a las herramientas de software. Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: <ul style="list-style-type: none"> Actividades asociadas a la administración de cuentas de usuario final (UserID). Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). Ejecución de comandos especiales sobre sistemas operativos. Ejecución de comandos especiales sobre bases de datos (dump, drop, delete, insert, update). Cambios de parámetros técnicos, de configuración o de seguridad. Cambios de configuración horaria. Cambios no autorizados en recursos tecnológicos críticos. Actividades de conexión de cuentas de usuario final o administradores. Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. Actividades asociadas a conexión de acceso remoto. Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional. La herramienta SIEM del Concejo de Bogotá D.C., será administrada y operada por el contratista, con personal con experiencia en servicios de monitoreo de logs. La actividad de monitoreo y alertamiento se debe hacer en las instalaciones del contratista. En caso de requerirse, el contratista deberá realizar las actividades necesarias de recuperación de credenciales de acceso, operación o administración del correlacionador de eventos y base de datos de logs. Las labores de configuración en el equipo SIEM de la Entidad y la generación de los casos de uso para el monitoreo SOC deberán ser ejecutadas por el personal asignado en el contrato. Deberá contener las etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que utilizará en la ejecución del contrato. Nota: El Concejo de Bogotá se reserva el derecho de ajustar aspectos de la metodología. Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario. Durante el período de la operación de los servicios se suministrará un esquema de escalamiento interno para la respuesta al mismo.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> El servicio debe garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoria y privacidad de los datos y servicios soportados. Las herramientas adicionales que deba utilizar el contratista, tales como hardware, software, firmware, utilitarios o appliances, deben cumplir con la regulación de derechos de autor y propiedad intelectual. Así mismo, deben contar con soporte, mantenimientos y actualizaciones del fabricante o proveedor y ser compatibles con la herramienta SIEM del Concejo de Bogotá D.C. El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el contratista deberá destruir toda la información a la que tuvo acceso del Concejo de Bogotá D.C. La configuración de cambios o requerimientos solicitados sobre la plataforma SIEM deberán ser gestionados en máximo 24 horas, previa aceptación de la ventana. Para casos de alta complejidad se definirán los tiempos específicos para estas configuraciones.
8.2	Monitoreo	<ul style="list-style-type: none"> El centro de monitoreo debe estar en la ciudad de Bogotá D.C. (Colombia). La conexión hacia la herramienta de correlación del Concejo de Bogotá se realizará a través de una conexión segura utilizando internet. El costo del canal de internet del contratista será asumido por él mismo. Cuando un evento de seguridad ocurre o está en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionarlo de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque. Detección de actividades, técnicas inusuales y recolección de evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo a los niveles de servicio. El servicio ofrecido deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por el Concejo de Bogotá D.C. El contratista deberá administrar la herramienta SIEM propiedad del Concejo de Bogotá, incluyendo la gestión de cambios y solución de problemas técnicos que se puedan presentar sobre la herramienta, de manera que se garantice la continuidad de la solución SIEM. Deberá mantenerse el inventario actualizado de dispositivos monitoreados de la solución. Las evidencias recopiladas por el servicio de monitoreo SOC son propiedad del Concejo de Bogotá D.C. y podrán ser solicitadas en cualquier momento para atención de requerimientos legales. SOC deberá analizar las diferentes alertas detectadas para descartar falsos positivos, antes de crear el caso/ticket en la herramienta institucional dispuesta para ello.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> Se debe poder realizar en forma remota y disponer de personal en sitio solo cuando sea necesario. Sincronización de 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/). Actividades permanentes para garantizar el descubrimiento y monitoreo de nuevos dispositivos en la red.
8.3	Incidentes	El contratista deberá entregar un informe preliminar de un incidente sucedido. Este debe ser remitido al Concejo de Bogotá D.C., posterior a la declaración del evento o incidente y después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.
8.4	Seguimiento	<ul style="list-style-type: none"> La actividad del servicio de monitoreo SOC, se centrará en el tratamiento de eventos, identificación de incidentes, los cuales contarán con un conjunto de metodologías y atención de procesos que permitirá brindar el alertamiento oportuno a los riesgos y amenazas. Adicionalmente realizará el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente. Apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información. Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo a las necesidades del Concejo de Bogotá, por ejemplo: <ul style="list-style-type: none"> - Alertas/Incidentes por tipo. - Alertas/Incidentes nuevos y resuelto. - Tiempo medio de creación de alertas/incidentes. - Tiempo medio de solución. - Tendencias y top de alertas/incidentes. - Cumplimiento de acuerdos de servicio. - Nivel de disponibilidad del servicio.
8.5	Certificaciones	<ul style="list-style-type: none"> Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por los modelos de procesos ITIL, CSIRT, ISO 27001:2022, ISO 20000:2018, NIST (CSF) o CERT. Nota: El contratista debe estar certificado en estas mejores prácticas de ISO 27001 e ISO 20000 para su proceso de SOC y deberá contar con Certificación vigente SOC 2 TYPE II. Los incidentes deben ser gestionados de acuerdo con las cinco fases de la ISO / IEC 27035: 2023: <ol style="list-style-type: none"> Planificar y preparar: establecer una política de gestión de incidentes de seguridad de la información y formar un Incident Response Team (Grupo de respuesta de incidentes). Detección e informes: El contratista deberá detectar e informar "eventos" que pueden ser o convertirse en incidentes. Evaluación y decisión: El contratista deberá evaluar la situación para determinar si de hecho se trata de un incidente.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>4. Respuestas: El contratista deberá reportar de manera oportuna al equipo de seguridad de Concejo de Bogotá D.C. para que pueda contener, erradicar y remediar.</p> <p>5. Lecciones aprendidas: El contratista deberá documentar la gestión de los riesgos de la información como consecuencia de las incidencias experimentadas.</p> <p>Nota: El contratista debe contar con certificado como miembro de FIRST durante toda la ejecución del contrato.</p> <ul style="list-style-type: none"> • ISO 27001: El oferente debe presentar junto con su propuesta el certificado ISO 27001 vigente para su proceso de SOC. • ISO 20000: El oferente debe presentar junto con su propuesta el certificado ISO 20000 vigente para su proceso de SOC. • FIRST: El oferente debe presentar junto con su propuesta el certificado de membresía de FIRST para su proceso de SOC. • SIEM personal: El oferente debe presentar una certificación emitida por el fabricante FORTINET de la solución SIEM que tiene el Concejo de Bogotá D.C. en operación, en la cual se certifique que cuenta con el personal técnico para la administración de la plataforma SIEM. • Proveedor certificado por fabricante de máxima categoría: El oferente deberá presentar certificado expedido por el fabricante FORTINET de la solución SIEM que tiene el Concejo de Bogotá D.C. en operación, en la cual se certifique que el oferente cuenta con el máximo nivel de membresía como canal proveedor de servicios. • CERTIFICACIÓN DE 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 los elementos relacionados en la ficha técnica de equipos tipo Firewall NGFW, en el máximo nivel de membresía en Colombia. Dicha certificación deberá ser expedida por el fabricante, la cual deberá estar dirigida a la entidad, con fecha no mayor a 30 días de expedida al cierre de la presentación de las ofertas • CERTIFICACIÓN DE ESPECIALIDADES: El oferente deberá allegar certificación expedida por el fabricante, para los elementos relacionados en la ficha técnica de equipos tipo Firewall NGFW donde acreditará que cuenta con mínimo cuatro (4) de las siguientes especialidades: (A) Operational Technology; (B) Public Cloud Security; (C) SD-WAN; (D) Security Operations; (E) SASE; (F) Secure Networking LAN; (G) Zero Trust Network Access (ZTNA); (H) Secure Networking Firewall.
8.6	Respuesta a incidentes	<ul style="list-style-type: none"> • Horario de atención 24x7 y los activos objeto de este servicio serán los mismos activos objeto del servicio de monitoreo SOC. • Proactivo, dependiente del servicio de monitoreo SOC. • Deberá contar con una línea de acceso telefónico o un buzón de correo para que el Concejo de Bogotá D.C. pueda solicitar la

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA "Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C."	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>atención y escalamiento correspondiente a este servicio cuando la entidad identifique que un evento de seguridad tenga lugar.</p> <ul style="list-style-type: none"> • El contratista deberá contar con un grupo interdisciplinario interno para la atención de incidentes de alto impacto con la aplicación de un procedimiento propio, claro y definido, el cual, deberá estar enfocado en las soluciones de seguridad del fabricante FORTINET que la Entidad tiene en operación. • Deberá alinearse a las políticas relacionadas con el intercambio seguro de información expedidas y/o aplicadas por el Entidad. • Deberá contar con un plan de respuesta a incidentes de seguridad de la información dependiendo del tipo de ataque y/o el tipo de vector utilizado. • Deberá tener desarrollados casos de uso estándar para los tipos de incidentes establecidos. • Definir escenarios de crisis para preparación ante amenazas persistente avanzadas (APT – por sus siglas en inglés, Advanced Persistent Threat), ataques de denegación de servicios (DDoS por sus siglas en inglés, Distributed Denial of Service) y ataques focalizados y, así, definir reglas para detectar, reaccionar y contener ataques dirigidos.
8.7	Registros y alarmas	<ul style="list-style-type: none"> • Personalización de reportes que el Concejo de Bogotá requiera durante la prestación del servicio. • Integración del envío de alarmas automáticas vía correo electrónico. • El servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo al Concejo de Bogotá D.C., resumiendo los resultados en boletines o informes extraordinarios de SOC. • Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior del Concejo de Bogotá D.C. • Se deberá generar un informe mensual de ejecución y prestación efectiva de los servicios de SOC. • Se deben generar alertas de otras amenazas que puedan impactar la infraestructura del Concejo de Bogotá, como las identificadas en los reportes de análisis de tendencia de centros SIRT/CERT o en las bases de datos de conocimiento del contratista. • Reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades del Concejo de Bogotá D.C.
8.8	Informes SOC	<ul style="list-style-type: none"> • El contratista deberá presentar informe mensual de monitoreo SOC, debe incluir:

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> - Estado y resultados del servicio en el periodo de valoración, de tipo gerencial. - Eventos de actividad sospechosa atendidos durante el periodo. - Alertas, ataques, incidentes y tendencias. - Comportamientos más relevantes según la correlación realizada por el contratista. - Incidentes de seguridad presentados. - Estadísticas de la información procesada. - Hallazgos realizados sobre la plataforma tecnológica. - Análisis y recomendaciones sobre los resultados. - Informe sobre la detección de vulnerabilidades a través de la herramienta de Gestión de Vulnerabilidades Continua. • El contratista integrará a los informes la inclusión de datos que el Concejo de Bogotá D.C., considere pertinentes, en la medida en que se vayan integrando nuevas herramientas. • El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el contratista deberá destruir toda la información a la que tuvo acceso del Concejo de Bogotá D.C. • El contratista debe informar al Concejo de Bogotá D.C. de manera inmediata, sobre cualquier evento o incidente real que se presenten en la infraestructura tecnológica. • La generación y envío de informes de servicio será realizada dentro de los primeros 5 días hábiles del mes. Los documentos entregables e informes que el contratista presente, deben contar con un formato de presentación estándar, redacción clara, buena ortografía y en idioma español.
8.9	Acuerdos de nivel de servicio	<ul style="list-style-type: none"> • Los servicios de Monitoreo SOC y Respuesta a Incidentes se realizarán en horario 7x24 durante toda la duración del contrato. • Ante la afectación de servicios se categorizarán los incidentes de acuerdo con lo siguiente: <ul style="list-style-type: none"> - Impacto crítico: Las plataformas cubiertas o la operación de la red o los servicios de TI que soportan la Corporación, administrados y configurados en las mismas, presentan pérdida de funcionalidad que afecta o comprometen la integridad, disponibilidad o confidencialidad de la información y han detenido dos o más operaciones del Concejo de Bogotá D.C. - Impacto alto: Las plataformas cubiertas o la operación de la red o los servicios de TI que soportan la Corporación, administrados y configurados en las mismas, presentan un desempeño inaceptable, degradado y tienen el potencial de comprometer la integridad, disponibilidad o confidencialidad de la información en las operaciones del Concejo de Bogotá D.C., o se encuentra detenida alguna de ellas. - Impacto moderado: Las plataformas cubiertas, alguno de sus componentes o la operación de la red o los servicios de TI que

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>soportan la Corporación, administrados y configurados en las mismas, se deteriora mientras las operaciones de la Corporación se mantienen funcionales.</p> <ul style="list-style-type: none"> - Impacto bajo: Se requiere información o asistencia en relación a capacidades, configuraciones, productos o servicios. Hay poco o nulo impacto en las operaciones de la Corporación. • Los reportes y monitorización de los servicios de SOC y Respuesta a Incidentes serán realizados con los tiempos de alertamiento y escalamiento al equipo de respuesta a incidentes, así: <ul style="list-style-type: none"> - De impacto crítico: alertamiento dentro de los primeros 30 minutos y escalamiento en máximo 1 hora. - De impacto alto: alertamiento dentro de los primeros 60 minutos y escalamiento en máximo 2 horas. - De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 12 horas. - De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 24 horas. • La configuración de cambios o requerimientos solicitados sobre la plataforma SIEM deberán ser gestionados en máximo 24 horas, previa aceptación de la ventana. Para casos de alta complejidad se definirán los tiempos específicos para estas configuraciones.
9. RECURSO HUMANO		
9.1	Equipo Mínimo de Trabajo.	<p>El contratista deberá realizar la instalación y configuración de los equipos con personal certificado en las plataformas ofertadas. Se deberá adjuntar certificación de fabricante que indique la ingeniería certificada asociada al proyecto, es decir que, las actividades de instalación, configuración y puesta en producción de las plataformas ofertadas deberán ser realizadas por personal certificado por el fabricante en la plataforma ofertada. Para lo cual se deberá adjuntar certificado vigente emitido por los fabricantes para el presente proceso.</p> <p>El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por:</p> <p><u>Gerente de servicio - Uno (1):</u></p> <p>Formación académica requerida: Título profesional de los núcleos básico de conocimiento (NBC) en ingeniería en electrónica, telecomunicaciones o afines; o ingeniería de sistemas, telemática y afines. Tarjeta o matrícula profesional, en los casos reglamentados por la ley. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, tarjeta o matrícula profesional y certificado de vigencia expedido por autoridad competente. Título de posgrado en Gerencia de Proyectos de</p>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<p>Ingeniería y/o Gerencia de Tecnología y/o Gerencia de proyectos en Tecnologías de la Información.</p> <p>Certificaciones vigentes: debe contar con mínimo seis (6) de las siguientes certificaciones:</p> <ul style="list-style-type: none"> • PMP (Project Management Professional). • CISM. • CEH. • ITIL v4. • IPV6 Básico LACNIC. • Security Sentinel. • Auditor líder ISO 27001:2022. • Auditor líder o interno ISO 22301:2019. • Scrum Foundation Professional Certificate (SFPC). • Scrum Foundation Fundamentals Certificate. <p>Experiencia General: Cinco (5) años, contados a partir de la fecha de expedición de la matrícula o tarjeta profesional.</p> <p>Experiencia específica: En proyectos relacionados con Seguridad de la Información, cuya duración acumulada mínima sea de tres (3) años o tiempo equivalente en el desarrollo de funciones similares, soporte y/o mantenimiento en soluciones de seguridad de la marca ofrecida. Para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia.</p> <p><u>Ingeniero de soporte y mantenimiento - Uno (1):</u></p> <p>Formación académica requerida: Título profesional de los núcleos básico de conocimiento (NBC) en ingeniería en electrónica, telecomunicaciones o afines; o ingeniería de sistemas, telemática y afines. Tarjeta o matrícula profesional, en los casos reglamentados por la ley. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, tarjeta o matrícula profesional y certificado de vigencia expedido por autoridad competente.</p> <p>Certificaciones vigentes: Debe contar con las siguientes tres (3) certificaciones o sus equivalentes ante el fabricante:</p> <ul style="list-style-type: none"> • Fortinet Certified Professional Network Security. • Fortinet Certified Professional Security Operations.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • Fortinet Certified Solution Specialist Network Security. • Fortinet Certified Solution Specialist Security Operations. <p>Experiencia General: Cuatro (4) años, contados a partir de la fecha de expedición de la matricula o tarjeta profesional.</p> <p>Experiencia específica: Tres (3) años de experiencia específica en instalaciones, soporte y/o mantenimiento en soluciones de seguridad de la marca ofrecida, para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia.</p> <p><u>Coordinador SOC – Uno (1):</u></p> <p>Formación académica requerida: Título profesional de los núcleos básico de conocimiento (NBC) en ingeniería en electrónica, telecomunicaciones o afines; o ingeniería de sistemas, telemática y afines, y/o título profesional en campos relacionados con electrónica, informática o tecnología. Tarjeta o matrícula profesional, en los casos reglamentados por la ley. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, tarjeta o matricula profesional y certificado de vigencia expedido por autoridad competente. Título en modalidad de especialización y/o maestría en Seguridad de la Información, y/o en general las que se relacionan claramente con seguridad de la información.</p> <p>Certificaciones vigentes: Debe contar con al menos cinco (5) de las siguientes certificaciones:</p> <ul style="list-style-type: none"> • The Center for Cybercrime Investigation & Cybersecurity Certificación: (FDDC) Foundations of Digital Defense and Cyberwarfare. • The Center for Cybercrime Investigation & Cybersecurity Certificación: (STACD) For attending the specialized training Advanced Cyber defender. • The Center for Cybercrime Investigation & Cybersecurity Certificación: (STOC) For attending the specialized training Offensive Cybersecurity. • EC-Council Certified Incident Handler v2 – ECIH. • ISO 27035 Gestión de incidentes de seguridad de la información. • Certified Information Security Management – CISM. • Auditor Líder ISO 27001:2022. • Certified Information Systems Auditor – CISA.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016


ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • PERITO CIBER JUDICIAL. Center for Cybercrime Investigation & Cybersecurity (Center for CIC). • Certified Ethical Hacker – CEH. • Ethical Hacking Professional Certification – CEHPC. • Certificación: CODSP (Certified Offensive and Defensive Security Professional). <p>Experiencia General: Cinco (5) años, contados a partir de la fecha de expedición de la matrícula o tarjeta profesional.</p> <p>Experiencia específica: Tres (3) años de experiencia específica en proyectos relacionados con seguridad de la información y/o seguridad informática como analista, ingeniero, coordinador, consultor, oficial y/o auditor de seguridad, para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia y formación.</p> <p><u>Analista de seguridad – Uno (1):</u></p> <p>Formación académica requerida: Título profesional de los núcleos básico de conocimiento (NBC) en ingeniería en electrónica, telecomunicaciones o afines; o ingeniería de sistemas, telemática y afines, y/o título profesional en campos relacionados con electrónica, informática o tecnología. Tarjeta o matrícula profesional, en los casos reglamentados por la ley. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, tarjeta o matrícula profesional y certificado de vigencia expedido por autoridad competente. Título en modalidad de especialización y/o maestría en Gerencia de Seguridad Informática y/o Administración de Riegos Informáticos y/o Gerencia de Proyectos de TI.</p> <p>Certificaciones vigentes: Debe contar con al menos cinco (5) de las siguientes certificaciones:</p> <ul style="list-style-type: none"> • Auditor Interno ISO 22301:2019. • Auditor Líder ISO 27001:2022. • EC-Council Certified Incident Handler v2 – ECIH • ISO 27035 Gestión de incidentes de seguridad de la información • Certified Information Security Management – CISM • Certified Information Systems Auditor – CISA • EC-Council Certified SOC Analyst 1 – CSA • Certified Ethical Hacker – CEH • Certified Digital Forensics Examiner CDFE • Computer Hacking Forensic Investigator – CHFI

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016

ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		<ul style="list-style-type: none"> • Offensive security Certified Professional – OSCP • Certified Network Defender – CND <p>Experiencia General: Cinco (5) años, contados a partir de la fecha de expedición de la matricula o tarjeta profesional.</p> <p>Experiencia específica: Cinco (5) años de experiencia específica en proyectos relacionados con seguridad de la información y/o seguridad informática como analista, coordinador, consultor, oficial y/o auditor de seguridad, para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia y formación.</p>
10. MANEJO DE RESIDUOS (Si aplica)		
<p>Realizar la gestión de todos los elementos, partes, desechos tecnológicos y residuos peligrosos que se generen durante la ejecución del contrato de acuerdo a lo establecido en la normatividad vigente, presentando previamente una carta o convenio actual entre el Proveedor y la empresa encargada del programa de disposición final presentado.</p> <ol style="list-style-type: none"> Debe presentar licencia ambiental de la empresa que realizará el tratamiento, aprovechamiento y/o disposición final según corresponda y cuando se realice la gestión el certificado de disposición final de los residuos en kilogramos. Realizar el pesaje y etiquetado del residuo peligroso generado de acuerdo a los lineamientos establecidos en la Corporación. Diligenciar la bitácora de generación de residuos peligrosos establecido por el Concejo cada vez que se realice el ingreso del residuo al área de almacenamiento de residuos peligrosos de la Corporación. Remitir de forma trimestral, registro de residuos peligrosos generados de forma mensual. Presentar las fichas de datos de seguridad de los insumos utilizados durante la ejecución del Contrato. Dar cumplimiento a lo establecido en el Decreto 1079 de 2015, en lo referente al transporte de mercancías peligrosas. Dar cumplimiento a los lineamientos establecidos en el plan institucional de gestión ambiental de la Corporación. 		
10.1	Residuos peligrosos	<p>El contratista está en la obligación de hacer la gestión integral de los residuos peligrosos RESPEL, de acuerdo con el Decreto 4741 de 2005 y Anexo 1 del mismo decreto, los cuales deben ser gestionados a través de una de las empresas gestoras de residuos peligrosos con licencia ambiental otorgada por una autoridad ambiental y al momento de la firma del acta de inicio debe presentar la copia de licencia vigente.</p> <p>En caso de que el contratista no cumpla directamente con este requisito podrá hacerlo a través de un tercero quien si cumpla con los requisitos para el manejo de los residuos tóxicos.</p>
10.2	Residuos de aparato	Para la gestión de RAEE (cableado, conectores, tomas eléctricas y los que se generen en ejecución del contrato), se deberá dar cumplimiento

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016

ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
	eléctricos y electrónicos	<p>a lo establecido en el Decreto 1076 de 2015, Título 7A, Capítulo IV de Disposiciones Finales de RAEE.</p> <p>Para la gestión de RAEE (cableado, conectores, tomas eléctricas y los que se generen en ejecución del contrato), se deberá dar cumplimiento a lo establecido en el Decreto 1076 de 2015, Título 7A, Capítulo IV de Disposiciones Finales de RAEE.</p> <p>De igual forma tendrá a su cargo que se realice la recolección, transporte y disposición final con empresas o entidades autorizadas por la autoridad competente, y presentará al supervisor del contrato copia de los formatos diligenciados del transporte y copia de la disposición de los residuos, dando cumplimiento a la normatividad vigente.</p> <p>El contratista deberá almacenar los residuos peligrosos generados en el área de almacenamiento que disponga el Concejo de Bogotá, dando cumplimiento a lo establecido en el plan de gestión integral de residuos peligrosos y deberá informar al responsable del Sistema de Gestión Ambiental del Concejo de Bogotá la fecha para el retiro de dichos residuos con el fin de realizar el acompañamiento de entrega de los residuos peligrosos y realizar lista de verificación del cumplimiento del Decreto 1609 de 2012 compilado en el Decreto 1079 de 2015 y/o la normatividad que le aplique.</p> <p>Los costos asociados o derivados del desarrollo de estas actividades serán asumidos por el contratista, quien también informara al funcionario responsable del programa de Gestión Ambiental de la Corporación, para que se lleve a cabo el registro de dicha gestión y la cuantificación de la generación del material asociado.</p> <p>En caso de que se generen residuos sólidos aprovechables durante la ejecución del contrato, estos deberán ser separados en la fuente por el contratista, labores que se efectuarán siguiendo el código de colores adoptado por la Corporación, en cumplimiento a lo establecido en el Plan Institucional de Gestión Ambiental.</p>
11. SEGURIDAD DE LA INFORMACIÓN		
11.1		El contratista debe salvaguardar la Confidencialidad, Integridad, Disponibilidad de la Información, de acuerdo a la política de Seguridad de la Información, Política de Protección de Datos Personales, para todos los activos que administre y/o maneje dentro del Concejo de Bogotá D.C., durante la vigencia del contrato, así como realizar la respectiva devolución de la información digital y/o física que le fue entregada al momento de iniciar el contrato y durante la vigencia del mismo hasta su finalización, por lo que se deberán acatar todas las directrices establecidas por el Concejo de Bogotá D.C. y el gobierno nacional, para el manejo seguro de la información.
11.2	Confidencialidad	El contratista y el personal que éste designe para realizar las diferentes labores en la Corporación deberán garantizar la confidencialidad de la información Institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución de las actividades, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SSI-PR005-FO1
	FICHA TÉCNICA “Prestar los servicios de administración, actualización, soporte técnico especializado, mantenimiento preventivo y correctivo incluyendo repuestos para los sistemas de ciberseguridad del Concejo de Bogotá D.C.”	VERSIÓN. No. 02
		FECHA: 30 MAR. 2016

ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
		Bajo ninguna circunstancia dicha información y/o documentación podrá ser utilizada por el proveedor o su personal para fines distintos al desarrollo de las actividades relacionadas con el presente contrato.

Proyectó: Carlos Andrés Padilla Pinto
Profesional Especializado
Oficina de Tecnología

Revisó: Alez Yobani Bociga Peña
Profesional Universitario
Oficina de Tecnología