ANEXO TÉCNICO

Adquirir la suscripción del servicio de EDR/XDR incluyendo soporte técnico, mantenimiento y actualización para los servidores que soportan la infraestructura del Icfes.

Septiembre de 2026

1 OBJETO A CONTRATAR

Adquirir la suscripción del servicio de EDR/XDR incluyendo soporte técnico, mantenimiento y actualización para los servidores que soportan la infraestructura del Icfes.

2 ALCANCE SERVICIO PARA LAS PRUEBAS DE SOFTWARE

Suministro de licenciamiento tipo SaaS para la solución de EDR/XDR (Endpoint Detection and Respond) para el Instituto Colombiano para la Evaluación de la Educación (ICFES).

EDR (Endpoint Detection and Respond)
El Instituto Colombiano para la Evaluación de la Educación (ICFES) requiere del licenciamiento de la solución EDR para 500 dispositivos.
La solución de EDR debe proporcionar al Instituto Colombiano para la Evaluación de la Educación (ICFES) un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas. La solución debe ser SaaS en su consola, no se aceptan soluciones en máquina virtual o físicas.
A continuación, se detallan y describen cada uno de estos mecanismos de protección requeridos:
Funcionalidades de Prevención
El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML)
Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube que se actualiza continuamente.
Proteger los endpoints desconectados de la red con una protección fuera de línea; este modo de operación se denomina modo autónomo.
Proporcionar un control de dispositivos USB basado en múltiples parámetros.
Debe estar en capacidad de eliminar tiempos de permanencia y Fatigas por exceso de alamas (falsos positivos)
Gestión de parches para sistemas operativos Windows, OS, Linux.
Funcionalidades de Descubrimiento
El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad
Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior
Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables
Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.
Funcionalidades de Detección y Protección.
El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o *file-less* y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado, debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de *ransomware*. Al mismo tiempo, el *backend* del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de

forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes así:
Se debe basar en la detección integrada de forma profunda en el sistema operativo, permitiendo las detecciones de ataques de infiltración sigilosa, los ataques basados en la memoria y los ataques “living off the land”.
Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).
Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa.
Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
Debe Permitir definir listas blancas y negras para personalizar mediante exclusiones estas protecciones (por hash, nombre y/o ruta de archivo, o por aplicación, incluyendo datos de versión y fabricante).
Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
Debe Proporcionar un análisis de todo el historial de eventos.
Debe realizar la validación continua de la clasificación de amenazas.
Funcionalidades de Protección contra Ransomware
La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo: 1. Debug de Procesos. 2. Código dinámico. 3. Formato de archivo ejecutable incorrecto 4. Una pila con código ejecutable 5. El programa ejecutado no tiene instalador 6. Programa crítico falso. 7. Empaquetador falso. 8. File Encryptor. 9. Proceso oculto. 10. Ejecutable inyectado. 11. Proceso inyectado. 12. Hilo inyectado. 13. Suma de comprobación no válida. 14. Ejecución no válida. 15. Puntero no válido. 16. Inyección de kernel. 17. Empaquetador conocido. 18. Archivo malicioso detectado. 19. Proceso malicioso. 20. Ejecutable modificado. 21. Stack Parcialmente asignado. 22. Exploit de escalamiento de privilegios. 23. Proceso vacío. 24. Manipulación de pilas. 25. Aplicación sospechosa. 26. Empaquetador sospechoso. 27. Ejecutable manipulado. 28. Ejecutable no confirmado. 29. Ejecutable sin asignar. 30. Código grabable.

Prevención automatizada en tiempo real encripción de Ransomware.
Funcionalidades de Remediación
La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando *playbooks* predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:
Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
Debe estandarizar los procedimientos de respuesta a incidentes con la automatización de playbooks
Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la apertura de tickets.
Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como, por ejemplo, grupos de estaciones de trabajo).
Debe proporcionar visibilidad completa de la cadena de ataque y los cambios maliciosos, mediante el seguimiento de código.
Debe permitir automatizar la limpieza y reversión de los cambios maliciosos preservando así la integridad del sistema.
Debe realizar la remediación, contención y respuesta de forma automática
Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
Funcionalidades de Investigación
Debe permitir automatizar la investigación, con una interrupción mínima para los usuarios finales en sus actividades de negocio, permitiendo realizar detallados análisis forenses sobre las amenazas detectadas y ataques desactivados en los dispositivos, recopilando información como ficheros y URLs accedidos, módulos cargados, procesos ejecutados, etc.
Debe desactivar y bloquear automáticamente las amenazas, lo que permite a los analistas de seguridad cazar marcando sus propios tiempos.
Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el “paciente cero”, incluso si el dispositivo está fuera de línea.
Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
La interfaz gráfica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.
Funcionalidades de EDR
La solución de EDR debe tener la capacidad de poder integrarse con diferentes plataformas de seguridad, creando así un marco robusto que pueda identificar y responder eficiente y eficazmente frente a los ataques como es recomendado por Gartner. La solución de EDR debe poder integrarse con las siguientes plataformas: 1. La solución EDR debe estar en capacidad de generar una acción de respuesta de incidente automática ante la detección de una IP maliciosa dirigida al Firewall directamente para realizar el correspondiente bloqueo. La configuración del playbook debe realizarse en la consola del EDR 2. La solución EDR debe estar en capacidad de generar una acción de respuesta de incidente automática ante la detección de un equipo comprometido dirigida al NAC directamente para realizar el correspondiente bloqueo 3. La solución EDR debe estar en capacidad de generar una acción de respuesta de incidente automática ante la detección de un archivo malicioso y dirigirlo directamente al Sandbox para su evaluación y clasificación. La configuración del playbook debe realizarse en el EDR 4. Capacidad de integración con solución de Deception 5. Capacidad de integración Correlacionador de Eventos, SIEM. 6. Capacidad de integración con Plataforma de Orquestación, automatización y respuesta a incidentes, SOAR. 7. Capacidad de integración con Plataforma de Análisis de comportamiento de usuario UEBA 8. La solución EDR debe estar en capacidad de generar una acción de respuesta de incidente automática dirigida al Directorio activo que pueda incluir el reset de la contraseña del usuario o deshabilitar la cuenta en el controlador de dominio dependiendo del tipo de evento.

Debe contar con una Gestión Unificada
Se debe incluir una asesoría y acompañamiento directo de fabrica por lo menos de 12 meses en los cuales se incluya asistencia directa en el diseño, planeación, playbooks, afinamiento de la solución, seguimiento semanal durante la implementación. Estas etapas deben ser realizadas directamente por parte del fabricante. No se admite que lo realice un partner o canal.
Debe contar con la funcionalidad de **IDENTIFICACIÓN DE INCIDENTES ENTRE PRODUCTOS**
Debe contar con la funcionalidad de **INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL**
Debe contar con la funcionalidad de **RESPUESTA AUTOMATIZADA**
El periodo de licenciamiento y soporte es de 12 meses a partir de la activación de las licencias.
Detección extendida sobre entornos de nube AWS
Detección extendida sobre entornos de nube Google
SERVICIOS PROFESIONALES Y DE SOPORTE REQUERIDOS
Generalidades:
El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
Instalación, Implementación, configuración y puesta en marcha de las soluciones de seguridad y conectividad ofertadas.
El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
El oferente debe presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto del fabricante: Gold, Premium, Expert o Platinum (según aplique al fabricante). Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad. esta certificación debe estar dirigida a la entidad y no debe superar los 30 días de expedición y se debe mencionar el objeto y numero del proceso.
El oferente debe presentar al menos CINCO (5) especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias Secure Networking Firewall, Secure Networking LAN Y Cloud Security o sus equivalentes. Esta certificación debe estar dirigida a la entidad y no debe superar los 30 días de expedición y se debe mencionar el objeto y numero del proceso.
En caso de uniones temporales y/o consorcios cada uno de los integrantes deberá aportar las certificaciones mencionadas en los requerimientos anteriores, con los mismos criterios y alcances mínimos establecidos para cada integrante del consorcio, no se realizará sumatoria y/o validación de tiempos de vigencia de las certificaciones para cumplir lo establecido.
El oferente debe entregar los documentos técnicos y/o datasheet del fabricante de las soluciones ofertadas, donde se evidencie el cummplimiento de cada uno de los ítems solicitados en los requerimientos técnicos de las soluciones.
El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil por el tiempo contratado.
Implementación y puesta en marcha solución de seguridad
El proponente seleccionado deberá entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas.
La implementación deberá contemplar:
· Planeación de cada una de las actividades, validadas en conjunto con el Instituto Colombiano para la Evaluación de la Educación (ICFES). Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas. · Afinamiento y estabilización de las plataformas. · Pruebas de Servicio de las plataformas. · Entrega de las plataformas a satisfacción del Instituto Colombiano para la Evaluación de la Educación (ICFES). Las actividades de afinamiento de la plataforma deberán ser realizadas por personal certificado por el fabricante
La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de la plataforma.

Soporte solución de seguridad

El contratista deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por un (1) año, con soporte remoto o en sitio en caso de requerirse.

El soporte deberá contemplar:

- El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas.
- Consultas a través de llamadas telefónicas, correo electrónico.
- Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil. Todo con respecto a las plataformas ofertadas y objeto del presente contrato

PRIORIDAD		DESCRIPCION
1	CRITICA	La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia
2	ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.
3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.
4	BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.

PRIORIDAD		DESCRIPCION
1	CRITICA	De manera remota (2) horas de atención y (3) horas de traslado a sitio.
2	ALTA	De manera remota (3) horas de atención y (4) horas de traslado a sitio.
3	MEDIA	De manera remota (8) horas y de ser necesario traslado a sitio
4	BAJA	De manera remota (24) horas y de ser necesario traslado a sitio

El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

- Revisar la consistencia de los Backups realizados a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita.
- Configurar, afinar y revisar los reportes / logs de las plataformas.

Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante

El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.

Se deben incluir en la oferta dos (02) actividades de mantenimiento preventivo y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.

El oferente debe contemplar una transferencia de conocimientos para 3 funcionarios de la entidad por 8 horas, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas.

Al finalizar cada visita correctiva y/o preventiva el contratista deberá:

- 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.

El oferente deberá consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración

El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.

Licenciamiento solución

El oferente deberá garantizar el licenciamiento del soporte y garantía por un periodo de un (1) año en un esquema 7x24 ante el fabricante a partir de la fecha de activación de las licencias en el portal del fabricante ofertado.

El oferente debe entregar al Instituto Colombiano para la Evaluación de la Educación (ICFES) un usuario de acceso al portal de los fabricantes de la solución, para la creación de casos, soporte de fábrica, actualización firmware de los dispositivos.

EQUIPO MINIMO DE TRABAJO REQUERIDO

Equipo	Titulo / Certificaciones / Cursos	Experiencia Profesional Especifica CUMPLE SI/NO
Un (01) Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de cinco (5) años Posgrado en Gerencia de Proyectos y/o Certificación PMP. Certificación Itil Foundation v3 o superior Certificación ITIL Managing Professional Certificacion Auditor Interno iso 27001	Experiencia mínima 10 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.
Un (01) Ingeniero Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación vigente en SCRUM Foundations Professional (SFPC) Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en implementación o administración en plataformas de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un (01) Ingeniero Implementador	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación en AUDITOR INTERNO en la norma ISO/IEC 27001:2022 Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente. Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en Nube emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de tres (5) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y/o monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un (01) Ingeniero de Soporte	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación en AUDITOR INTERNO en la norma ISO/IEC 27001:2022 Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de tres (5) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y/o monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

	Certificación vigente como Arquitecto o Experto o su equivalente en seguridad de Operaciones emitida por el fabricante con el cual se está presentando el proponente.		
Nota: El personal de técnico requerido debe ser propio del oferente, no se aceptan figuras de tercerización de servicios o prestación de servicios, para ello se deberán enviar las hojas de vida y/o contrato de vinculación laboral en conjunto con la propuesta, una vez se suscriba el acta de inicio.			

CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN

- Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato. El contratista deberá asegurar el cuidado, la confidencialidad y la correcta utilización de la información entregada y generada durante la duración de la garantía, soporte y mantenimiento del contrato, así como de los elementos que para su ejecución el Instituto ponga a su disposición.

- De igual manera, de los afinamientos, las políticas y los procesos en la actualización de la solución serán considerados por el contratista como información confidencial propiedad del Instituto Colombiano para la Evaluación de la Educación – Icfes, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.

- Durante los afinamientos, actualización y soporte de las herramientas, el contratista se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.

Robinson Rivera Cardona
Director de tecnología e Información (E)

ACCIÓN	RESPONSABLE	CARGO	FIRMA
Elaboró	**Diego Mauricio Salas**	Subdirector de Información	