ANEXO TÉCNICO

OPERACIÓN DEL EQUIPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA COLCERT

OBJETO: Prestación de servicios orientados a apoyar la ejecución técnica y operativa de las actividades del Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT/CSIRT Gobierno), mediante la implementación de soluciones tecnológicas, así como la provisión de servicios expertos.

Contenido

1. DEFINICIONES TÉCNICAS ESENCIALES

CERT Nacional: Un CERT (Computer Emergency Response Team) Nacional es un equipo especializado que proporciona asistencia y respuesta a incidentes de seguridad informática a nivel nacional. Su función principal es coordinar y gestionar incidentes de ciberseguridad, proporcionar orientación a los organismos gubernamentales y al sector privado sobre la seguridad informática, y fomentar la colaboración entre diferentes partes interesadas. (Kossakowski, K., & Szewczyk, R. (2015). "National Computer Security Incident Response Teams (CSIRTs): Overview and Key Recommendations". ENISA. ENISA - National CSIRTs)

CSIRT de Gobierno: Un CSIRT (Computer Security Incident Response Team) de Gobierno es un equipo específico dentro de la administración pública que se centra en responder a incidentes de seguridad cibernética que afectan a las instituciones gubernamentales. Su labor incluye la detección, análisis, mitigación y respuesta a incidentes, así como la divulgación de información y la capacitación en ciberseguridad. (Federal Trade Commission (FTC). "Cybersecurity for the Government: A Guide for the Public Sector". FTC Cybersecurity Guide)

ColCERT: Grupo Interno de Trabajo Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, es el CERT Nacional de Colombia y actúa como el punto central de coordinación a nivel nacional para la gestión de amenazas e incidentes de seguridad digital, colaborando con otros CSIRTs, entidades públicas y privadas; facilita la respuesta rápida y eficiente a incidentes y vulnerabilidades; apoya a las entidades públicas en la mejora de su ciberseguridad; promueve la creación de CSIRTs sectoriales; desarrolla y divulga guías y recomendaciones de seguridad; y coordina la identificación y protección de infraestructuras críticas.

SOC (Security Operations Center): Un SOC (Security Operations Center) es una instalación centralizada que se encarga de la supervisión, detección, respuesta y gestión de incidentes de ciberseguridad en tiempo real. Los SOC utilizan tecnologías avanzadas, como SIEM (Security Information and Event Management), para analizar y correlacionar datos de seguridad, permitiendo una respuesta rápida ante amenazas. (NIST (National Institute of Standards and Technology). "Guide to Cyber Threat Information Sharing". NIST Special Publication 800-150. NIST Guide)

SOC ColCERT: El centro de operaciones de ciberseguridad (SOC) del ColCERT, es una iniciativa para el fortalecimiento de capacidades técnicas del ColCERT, permitiendo combinar el uso de herramientas tecnológicas para realizar inteligencia de amenazas, apoyar la gestión de incidentes de seguridad digital y apoyar los servicios del portafolio con herramientas y soluciones de ciberseguridad, para hacer frente a las amenazas, riegos y vulnerabilidades en seguridad digital que puedan afectar la continuidad de la operación de entidades públicas y privadas a nivel nacional. De esta forma se busca cumplir con la misionalidad y las obligaciones establecidas en el Decreto 338 de 2022 y la Resolución 500 de 2021, las cuales exigen ofrecer un amplio portafolio de servicio para las diferentes entidades en cumplimiento de dichos lineamientos y el cierre de la brecha en seguridad digital que debe proveer e impulsar el estado.

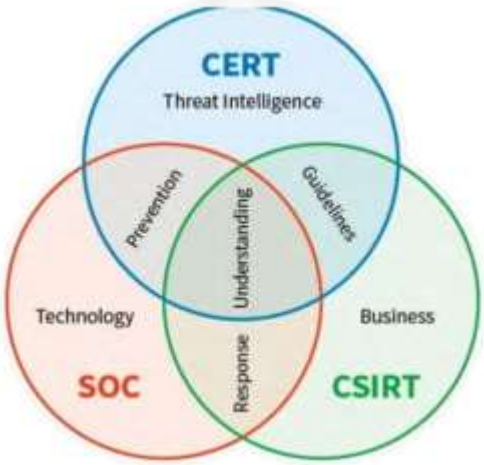

Imagen 1: Relación CERT/CSIRT/SOC Fuente: Exabeam

2. CONTEXTO TÉCNICO.

La complejidad creciente de las amenazas cibernéticas subraya la prioridad esencial de la Seguridad Digital/Ciberseguridad para gobiernos y organizaciones en todo el mundo. La protección de infraestructuras tecnológicas y críticas, la información sensible y la garantía de la continuidad operativa ante posibles incidentes demandan el desarrollo y la implementación de estrategias de seguridad digital continuas y, fundamentalmente, capacidades técnicas y humanas especializadas. El ColCERT se erige como un actor clave en este escenario, desplegando estas capacidades vitales en entidades públicas y privadas para la prevención y gestión de incidentes, el cierre de la brecha digital, la transferencia de conocimiento y la identificación de infraestructura crítica y servicios esenciales.

El CERT Nacional actúa como punto focal de respuesta a incidentes de seguridad digital a nivel nacional, tiene como misión dirigir y coordinar la gestión de incidentes cibernéticos que afecten la seguridad digital nacional. Esto implica proporcionar asistencia técnica especializada y directrices no solo a entidades gubernamentales y al sector privado, sino también establecer los lineamientos para la operación de los CSIRT sectoriales y territoriales. Asimismo, fomenta la colaboración y el intercambio de información sobre amenazas y vulnerabilidades, definiendo los mecanismos para esta compartición, contribuyendo así a fortalecer la resiliencia cibernética del país de manera integral y coordinada.

Por otro lado, el **CSIRT de Gobierno** está enfocado en las necesidades específicas del sector público. Este equipo se especializa en detectar, analizar y responder a incidentes de seguridad que afectan a las instituciones gubernamentales. El CSIRT se encarga de proteger la integridad y disponibilidad de los servicios, así como de asegurar la confianza de los ciudadanos en las plataformas digitales del gobierno.

Finalmente, el **SOC** optimiza las capacidades técnicas del ColCERT al unificar el uso de herramientas tecnológicas especializadas en inteligencia de amenazas y gestión de incidentes de seguridad digital. Esta integración, junto con el apoyo de soluciones de ciberseguridad para los servicios del portafolio, permite al ColCERT abordar de manera integral las amenazas, riesgos y vulnerabilidades que puedan afectar la continuidad operativa de las organizaciones públicas y privadas en todo el país.

En conclusión, la defensa integral contra amenazas, riesgos y vulnerabilidades cibernéticas se fundamenta en la articulación de las funciones del ColCERT como CERT Nacional, su apoyo en la coordinación de incidentes a entidades públicas y privadas, y las capacidades técnicas de su portafolio de servicios. No obstante, el **equipo técnico especializado** es el pilar fundamental de esta defensa, ya que su conocimiento y experiencia son esenciales para gestionar las herramientas y desplegar los servicios del portafolio, garantizando así la entrega efectiva de valor a las organizaciones para fortalecer sus posturas de seguridad.
para garantizar cada unoa de los

3. OBJETO

Prestación de servicios orientados a apoyar la ejecución técnica y operativa de las actividades del Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT/CSIRT Gobierno), mediante la implementación de soluciones tecnológicas, así como la provisión de servicios expertos.

4. JUSTIFICACIÓN

Según lo definido en el Decreto 338 de 2022, el Equipo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT paso de estar adscrito al Ministerio de Defensa y pasar como Grupo Interno de trabajo de la entidad designada por la Corporación, específicamente al Despacho del Viceministro de Transformación Digital. Esta transición se formalizo también en la estructura de los grupos internos de MinTIC a través de la Resolución 3066 de 2022 mediante la cual se creó el grupo de trabajo al interior de esta entidad designada por la Corporación. En línea con lo descrito, es importante señalar que dentro de las disposiciones de dicha Resolución se asignaron a este grupo de trabajo las funciones propias de CSIRT Gobierno el cual opera dentro del alcance del ColCERT.

En el marco del contrato de compraventa No. 766-2022, se adquirieron capacidades tecnológicas esenciales para la operación y el fortalecimiento del Centro de Respuesta a Incidentes de Seguridad Cibernética del Gobierno (CSIRT Gobierno), ahora integrado y ampliado bajo el Equipo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT. La adquisición de estas herramientas permitió ampliar las capacidades técnicas para soportar las actividades del portafolio de servicios que se ofrecen a las entidades gubernamentales y al sector privado colombiano, en su rol como CERT Nacional de Colombia. La adquisición de estas herramientas fue fundamental para mantener y expandir los servicios críticos que el ColCERT presta a nivel nacional.

Así las cosas, en el desarrollo de este contrato se adquirieron herramientas esenciales para las operaciones del ColCERT, incluyendo Tenable para análisis de vulnerabilidades, la Sandbox DoD de Trellix para análisis de malware, Mandiant para inteligencia de amenazas, la solución EDR de Trellix para protección de endpoints, Cisco Umbrella para investigación de DNS y seguridad web, Manage Engine para validación de disponibilidad de sitios web, Mailchimp para envío de correo masivo y la solución Totemomail para el cifrado y descifrado de correos, fortaleciendo integralmente las capacidades de detección, prevención, respuesta y comunicación del CERT Nacional.

Con el objetivo de asegurar la continuidad de las operaciones y el despliegue del portafolio de servicios ofrecido por el ColCERT, en el año 2023 se formalizó el Contrato 1307. A través de éste, se llevó a cabo la renovación de las herramientas previamente adquiridas mediante el contrato 766-2022. Dicha renovación posibilitó el mantenimiento ininterrumpido de los servicios de análisis situacional, la gestión de vulnerabilidades, la gestión de incidentes y la transferencia de conocimiento a entidades gubernamentales y privadas a nivel nacional, Sin embargo, el licenciamiento de estas herramientas, con una vigencia de dieciocho (18) meses, expira en junio de 2025, haciendo necesaria su renovación para asegurar la continuidad de las operaciones del ColCERT.

En el año 2024, el Fondo Único de Tecnologías de la Información y las Comunicaciones adquirió una capacidad instalada con la suscripción del contrato interadministrativo No. 2144-2024 con la Corporación Colombia Digital, mediante la implementación de nuevas herramientas tecnológicas avanzadas en ciberseguridad, adicionales a las adquiridas en el contrato 1307 del 2023. Esta inversión permitió ampliar las capacidades técnicas del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, para soportar las operaciones de SOC, desplegadas mediante el portafolio de servicios.

Así las cosas, resulta crítico renovar las licencias de las herramientas de seguridad adquiridas en 2023 (Contrato 1307), cuyo vencimiento se aproxima en junio. Sin esta renovación por doce (12) meses, se interrumpiría la continuidad de servicios esenciales como el análisis de vulnerabilidades, el análisis situacional y la gestión de incidentes. Esta renovación es precedente fundamental para poder aprovechar la contratación de personal técnico especializado, quienes serán esenciales para operar eficientemente tanto estas herramientas actuales como las nuevas capacidades técnicas que se planean adquirir en 2025.

La contratación de personal técnico especializado es una necesidad apremiante para maximizar el valor de las inversiones tecnológicas realizadas en 2023 y para la puesta en marcha y operación efectiva de las nuevas herramientas que se adquirirán en 2025. Estos profesionales serán la fuerza operativa que permitirá expandir significativamente la cobertura de los servicios del ColCERT a entidades públicas y privadas, entregando información estratégica para fortalecer su seguridad, cerrar la brecha digital, fomentar una cultura de ciberseguridad y mejorar la respuesta ante incidentes. Sin la renovación de las licencias existentes, la incorporación de este personal no podría desplegar las líneas del portafolio de manera efectiva.

La eficiente operación y el máximo aprovechamiento de las capacidades técnicas, tanto las actuales (2023) como las futuras (2025), dependen directamente de la disponibilidad de personal técnico especializado. Estos profesionales transformarán las funcionalidades de las herramientas en inteligencia de valor para la protección del ecosistema digital

colombiano. Sin embargo, esta capacidad operativa se vería severamente limitada si no se realiza la renovación de las licencias de las herramientas de 2023 que vencen en junio, impidiendo la continuidad de las operaciones base sobre las cuales se apalancará el trabajo del nuevo personal y la implementación de las nuevas herramientas.

Por lo tanto, la renovación de las licencias existentes es una condición indispensable para garantizar la continuidad operativa del ColCERT y para poder integrar y utilizar eficazmente el personal técnico especializado que se contratará. Este equipo humano será fundamental para operar las herramientas actuales y las nuevas adquisiciones de 2025, permitiendo así la expansión de la cobertura de los servicios, la generación de información predictiva para la prevención de incidentes y el fortalecimiento de la ciberseguridad a nivel nacional. Sin la renovación de las licencias de 2023, la inversión en nuevo personal y futuras herramientas no podría alcanzar su máximo potencial.

En definitiva, la acción coordinada de renovar las licencias de las herramientas de 2023 y contratar personal técnico especializado es crucial para el futuro del ColCERT. Sin la renovación, la inversión en personal y futuras herramientas (2025) se vería comprometida, impidiendo la continuidad de los servicios actuales y la expansión de la cobertura. Con ambos elementos en su lugar, el ColCERT estará en capacidad de gestionar eficazmente las herramientas instaladas y las venideras, generando información predictiva vital para anticipar y mitigar amenazas, incluyendo los desafíos planteados por tecnologías emergentes. Este fortalecimiento posicionará a Colombia como un líder en ciberseguridad, protegiendo su infraestructura digital y su ciudadanía de manera integral.

5. PORTAFOLIO DE SERVICIOS ColCERT

El ColCERT actúa como el único punto de contacto tanto a nivel nacional como internacional para la gestión de incidentes de seguridad digital (Ciberseguridad) en Colombia. Además, coordina las instancias responsables de la seguridad digital, incluyendo los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) sectoriales, tanto públicos como privados. Ofrece un portafolio de servicios que se divide en cuatro líneas específicas: análisis situacional, gestión de vulnerabilidades, gestión de incidentes y transferencia de conocimiento (ver Imagen No. 1).

Imagen 1. Portafolio de Servicios

COLCERT – www.ColCERTgov.co

En este contexto, el ColCERT, dispone de diversas herramientas de seguridad e infraestructura tecnológica para desarrollar y desplegar sus servicios. Estas herramientas cuentan con licencias válidas hasta junio y diciembre del 2025. Además, la gestión de su infraestructura on- premise es llevada a cabo por personal técnico especializado del Equipo COLCERT

Para desarrollar cada uno de los servicios del portafolio, el ColCERT ofrece a las entidades públicas y privadas los siguientes servicios:

- Generación de Alertas y Advertencias / Observatorio de Seguridad Digital: incluye Informes Coyunturales, Informes Estratégicos e Informes Técnicos.

- Gestión de Vulnerabilidades: Incluye análisis de infraestructura on premise, web, nube y directorio activo Vulnerabilidades WEB y Divulgación y Respuesta a Vulnerabilidades.

- Gestión de Incidentes: Apoyo y coordinación en gestión de incidentes de seguridad digital a las entidades públicas y privadas.

- Transferencia de Conocimiento: mediante la concientización de funcionarios, contratista y colaboradores en seguridad digital y capacitación en gestión de incidentes.

Además, el ColCERT ofrece sus servicios a 10 comunidades específicas: Para más detalles, ver Imagen No. 2.

1. Rama Ejecutiva
2. Rama Legislativa
3. Rama Judicial
4. Fuerzas Militares
5. CSIRT Sectorial

6. CSIRT Privado
7. Instancia Ciber
8. Sector Privado
9. Pymes
10. Sociedad Civil

Imagen 2. Comunidades a la cuales el COLCERT ofrece sus servicios

6. ALCANCE DE LA NECESIDAD:

Con el objetivo de entregar eficazmente los servicios actuales derivados del despliegue de las herramientas y soluciones de seguridad digital, desde el equipo ColCERT se genera la necesidad de atender un proyecto de fortalecimiento de sus capacidades desde el punto de vista de prestación de servicios y de infraestructura, para el desarrollo de este proyecto se estructura a través de cuatro (4) fases de la siguiente forma:

1. Fase I: Planificación y Preparación

En esta fase, se define la metodología de gestión y seguimiento del proyecto. Se elabora un cronograma de actividades y se conforman equipos técnicos especializados para desarrollar cada línea específica del proyecto. Además, se articulan los equipos técnicos del ColCERT con los líderes técnicos según la sección de equipo de trabajo.

2. Fase II: Desarrollo de Capacidades y Renovación

Esta fase se centra en la gestión e implementación de las soluciones. Incluye el licenciamiento de las herramientas identificadas por el equipo ColCERT, la configuración y puesta en marcha de herramientas renovadas, y la validación de certificaciones vigentes emitidas por el fabricante o un organismo de certificación reconocido. También se realiza el entrenamiento en el uso de herramientas del equipo ColCERT por personal especializado.

3. Fase III: Fortalecimiento de las Capacidades de Despliegue

En esta fase, se despliegan las líneas de operación del catálogo de servicios del ColCERT. Se elabora un plan de trabajo con metodología de comunicación y canales para la entrega de insumos. Se realizan análisis situacionales, análisis de vulnerabilidades, y se generan informes de resultados de los servicios de análisis de vulnerabilidades e inteligencia de amenazas solicitados por el ColCERT. Además, se proporciona apoyo a la gestión de incidentes y se documentan las actividades solicitadas por el ColCERT.

4. Fase IV: Diseño de Material Comunicacional

Esta fase se enfoca en la producción audiovisual. Incluye la creación de videos informativos y promocionales, la edición y postproducción de contenido, y la implementación de campañas de comunicación. Se difunde el catálogo de servicios en coordinación con el MINTIC y se utilizan diversos canales de comunicación para la divulgación de los servicios del ColCERT.

Por otro lado, el proyecto se desarrollará en 4 líneas de trabajo, por ejemplo para el desarrollo de la **línea No.1**, el cooperante deberá **conformar equipos técnicos especializados para desarrollar líneas específicas del portafolio de ColCERT**. Estos equipos operarán bajo un esquema 5/8 y en coordinación con el equipo de ColCERT para asegurar la correcta implementación de los servicios. La información procesada y gestionada internamente proporcionará inteligencia oportuna y dinámica sobre amenazas, riesgos y vulnerabilidades, permitiendo a las organizaciones fortalecer su seguridad tecnológica en infraestructuras locales y en la nube.

En la **línea No. 2**, el cooperante se compromete a **realizar la renovación de las licencias** por un plazo no menor a 12 meses de las herramientas identificadas por el equipo ColCERT.

Para las **líneas 3 y 4**, además, se establecerá un equipo central altamente capacitado que será responsable de liderar y coordinar todas las actividades acordadas en estrecha colaboración con el equipo de la entidad designada por la Corporación. Este equipo tendrá la tarea de desarrollar y diseñar el material audiovisual necesario para la promoción y despliegue de las actividades tácticas.

El equipo central no solo se encargará de la creación de contenido audiovisual de alta calidad, sino que también garantizará que dicho material cumpla con los estándares y directrices establecidos por el MINTIC. Esto incluirá la planificación estratégica, la producción de videos informativos y promocionales, la edición y postproducción de contenido, así como la implementación de campañas de difusión a través de diversos canales de comunicación.

Todo esto con el objetivo de asegurar que el material audiovisual sea efectivo en comunicar los mensajes clave y en alcanzar los objetivos de las actividades tácticas planificadas. En resumen, este equipo central será fundamental para el éxito del proyecto, proporcionando una dirección clara y una ejecución impecable en todas las fases del desarrollo y diseño del material audiovisual necesario para la promoción y despliegue de las actividades tácticas.

Los servicios de análisis situacional y las demás líneas del portafolio de ColCERT deben ejecutarse en estricta conformidad con las buenas prácticas y a los procedimientos, guías y protocolos establecidos por el ColCERT. El cooperante deberá adoptar e implementar conjuntamente aquellos que sean necesarios para asegurar la correcta gestión y operación de cada servicio.

En resumen, este proyecto se estructurará en cuatro fases principales con líneas de servicio específicas para asegurar una implementación eficaz y coordinada de todas las actividades planificadas.

7. EQUIPO DE TRABAJO BASE

El cooperante seleccionado debe contar con un equipo de trabajo base multidisciplinario altamente calificado, con perfiles específicos orientados a satisfacer las necesidades de cada uno de los componentes del proceso, de esta manera se deberán asignar líderes direccionados a cada línea de servicio y quienes realizarán la gestión de coordinación directa con el equipo de ColCERT. A continuación, se detallan los perfiles mínimos requeridos durante la ejecución del contrato; cada uno con sus respectivas certificaciones y experiencia, los cuales deben tener una dedicación del 100% y disponibilidad permanente:

PERFIL	EXPERIENCIA	EXPERIENCIA ESPECIFICA
Gerente de Proyectos	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. • Especialista en Gerencia de proyectos • PMP • Scrum Master • Lead Risk Manager ISO 31000 • Lead Implementer ISO 27001:2022	Experiencia como Gerente de proyectos de seguridad de la información o seguridad informática de por lo menos dos (2) años.
Consultor de seguridad I	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. • Lead CyberSecurity Professional Certification - LCSPC • Auditor Líder ISO 27001:2022 • Lead Implementer ISO 27001:2022 • Certified Ehtical Hacker- EC-Council	Experiencia como consultor de seguridad de la información o seguridad informática de dos (2) años.

PERFIL	EXPERIENCIA	EXPERIENCIA ESPECIFICA
	• Cyber Security Foundation Professional Certificate – CSFPC • Scrum Master • ISO 22301:2019 Auditor interno • CISM-Certified Information security manager • Artificial Intelligence Expert Certificate -CAIEC	
Consultor de seguridad II	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. • Lead CyberSecurity Professional Certification - LCSPC • Auditor Líder ISO 27001:2022 • Cyber Security Foundation Professional Certificate – CSFPC • Ethical Hacking Professional Certification CEHPC • CISM-Certified Information security manager • Artificial Intelligence Professional Certificate -CAIPC	Experiencia como director o coordinador o consultor de seguridad de la información o seguridad informática de dos (2) años.
Especialista en Inteligencia de amenazas	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. Certificaciones en: • Auditor interno ISO 27001:2022 • Certified Threat Intelligence Analyst	Experiencia en inteligencia de amenazas y/o seguridad en ciberdefensa de por lo menos 3 años
Consultor de seguridad III	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática.Especialización en auditoria de sistemas Certificaciones en: • Lead Risk Manager ISO 31000	Experiencia en seguridad informática de tres (3) años y por lo menos un año de experiencia en labores relacionas con SOC

PERFIL	EXPERIENCIA	EXPERIENCIA ESPECIFICA
	• Auditor ISO 19011:2018 • Lead Cybersecurity Manager NIST CSF 2.0 • Lead Cybersecurity Manager ISO 27032:2023 • Lead Auditor ISO 27701:2019 • Lead Auditor ISO 22301:2019	

8. LÍNEAS DE SERVICIO

8.1. Capacidades de despliegue del catálogo de servicios del equipo ColCERT.

4.1 Línea Análisis Situacional

La efectividad del CERT nacional en la protección del ciberespacio y la prevención de incidentes de seguridad digital depende en gran medida de un servicio de análisis situacional continuo y de alta calidad, este servicio proporciona la inteligencia necesaria para comprender el panorama de amenazas y fundamentar las decisiones estratégicas de seguridad. En este sentido, se requiere que el cooperante garantice la operación permanente de este servicio, a través de un centro de operaciones, ubicado en un espacio de trabajo seguro, y dotado con los recursos tecnológicos y humanos necesarios para asegurar la continuidad operativa durante toda la duración del contrato.

En el siguiente cuadro de detallan los requerimientos mínimos que debe ser cumplidos por el cooperante para garantizar la correcta ejecución de esta línea de trabajo.

ITEM	DESCRIPCIÓN
1.	El cooperante debe conformar un equipo de especialistas y analistas en ciberseguridad que trabajará de manera conjunta y coordinada con el equipo técnico del ColCERT.
2.	El cooperante debe realizar un monitoreo permanente a amenazas, riesgos, vulnerabilidades, IoC e Información relacionada con ciberseguridad, que pueda generar incidentes o un impacto en las operaciones de las entidades públicas y privadas en Colombia.
3.	Para la entrega de alertas, advertencias, informes y boletines, el cooperante deberá implementar y ejecutar las fases del Ciclo de Vida de la Inteligencia de Amenazas (CTI), asegurando que toda la información proporcionada haya sido debidamente procesada y analizada para su validez y relevancia.

ITEM	DESCRIPCIÓN
4.	El cooperante debe hacer la gestión de alertas y eventos en tiempo real, clasificando y priorizando amenazas según su impacto.
5.	El cooperante debe realizar un monitoreo continuo de indicadores de compromiso (IOCs) que aporten en el cierre de brechas de entidades gubernamentales u organizaciones de los sectores críticos del país.
6.	El cooperante debe realizar informes de tendencias y amenazas actuales.
7.	El cooperante debe realizar la implementación de alertas proactivas basadas en inteligencia de amenazas.
8.	El cooperante debe desarrollar estrategias de defensa adaptativa ante nuevas amenazas.
9.	El cooperante deberá realizar un análisis específico para cada sector de infraestructura crítica identificado, con el objetivo de determinar los Grupos de Amenaza Persistente Avanzada (APT) que representan una amenaza potencial de ciberataque. Para este análisis, se utilizarán los marcos de referencia MITRE ATT&CK y Cyber Kill Chain, lo que permitirá identificar tendencias, tácticas, técnicas y procedimientos (TTPs) empleados por estos actores de amenaza. Con base en este análisis, el cooperante generará un modelo de amenazas para cada sector, alineado con las mejores prácticas de la industria.
10.	El cooperante debe hacer la identificación de campañas de phishing dirigidas contra entidades públicas y privadas.
11.	El cooperante debe realizar caza de amenazas (Threat Hunting) para identificar ataques activos en la infraestructura de entidades públicas y privadas.
12.	El cooperante debe desarrollar informes de inteligencia de amenazas según los formatos establecidos por el Equipo ColCERT, con tendencias y predicciones basadas en datos históricos.
13.	El cooperante debe apoyar al ColCERT en la generación, monitoreo y análisis de indicadores, métricas y metas en materia ciberseguridad, a nivel estratégico, táctico y operativo, asegurando su medición y evaluación periódica, para la toma de decisiones.
14.	El cooperante debe llevar a cabo las tareas o actividades de CTI basándose, entre otras en: **Superficie de Ataque (Entidades Públicas y Privadas):** • Monitoreo continuo de diversas fuentes de información: • Feeds de inteligencia de amenazas. • Herramientas internas del ColCERT. • Boletines de organismos internacionales. • Cooperantees especializados en ciberseguridad. • Información compartida por SOC/CSIRT/PSIRT a nivel local, regional y global. **Proceso de Análisis y Entrega de Información:** • **Revisión y Afinamiento:** Optimización continua de las herramientas de Inteligencia de Amenazas (CTI) y Plataformas de Inteligencia de Amenazas (TIP), incluyendo la instancia MISP del ColCERT.

ITEM	DESCRIPCIÓN
	• **Evaluación:** Análisis exhaustivo de amenazas, riesgos y vulnerabilidades, siguiendo el ciclo de vida de la información de CTI. • **Entrega:** Diseminación de información procesada y accionable para la elaboración de alertas, boletines y advertencias dirigidas a las entidades públicas y privadas.
SERVICIO CYBER THREAT INTELLIGENCE & RISK ASSESSMENT (CTIRA)	
15.	El cooperante establecerá un proceso proactivo y continuo para identificar y rastrear amenazas, riesgos, vulnerabilidades e incidentes de ciberseguridad reportados por el ColCERT, complementado con la validación de información y la detección de filtraciones de datos en la "internet profunda". Esta estrategia permitirá anticipar posibles ataques contra entidades públicas y privadas, facilitando la implementación de medidas preventivas oportunas.
16.	El cooperante debe realizar la monitorización sobre los contenidos públicos, ocultos y sobre aquellos que no sean legítimos, con un enfoque claro y orientado a la detección de amenazas incluido Phishing.
17.	El servicio de Cyber Threat Intelligence & Risk Assessment (CTIRA) deberá implementar rigurosamente cada una de las fases del procesamiento de la información de CTI para garantizar la generación de inteligencia confiable y confirmada sobre amenazas y riesgos.
18.	El servicio de Cyber Threat Intelligence & Risk Assessment (CTIRA) deberá llevar a cabo la identificación de dominios pertenecientes a entidades gubernamentales y privadas con el fin de detectar y analizar posibles abusos de DNS.
19.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) deberá contar con Monitorización de Fugas de Información, esta fuga de información puede referirse a la filtración deliberada o involuntaria de información confidencial o sensible de entidades de gobiernos y privadas de los sectores críticos que llega a conocimiento de terceras personas ajenas a la entidad.
20.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) debe evaluar, visualizar y mejorar la postura de seguridad de las entidades de publicas y privados a través de métricas continuas y calificaciones por dominio de seguridad.
21.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) debe hacer la recolección y análisis de datos públicos de ciberseguridad de entidades de publicas y privado
22.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) debe realizar el monitoreo continuo de direcciones IP por actividad sospechosa o maliciosa identificadas.
23.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) debe elaborar de informes mensuales de evolución del score de seguridad.
24.	El servicio Cyber Threat Intelligence & Risk Assessment (CTIRA) debe realizar análisis de tendencias, TTP. riesgos emergentes y amenazas.

4.2 Línea Gestión de vulnerabilidades

La gestión de vulnerabilidades es crucial para la continuidad operacional de entidades públicas y privadas. Implica identificar debilidades con herramientas del ColCERT y fuentes abiertas, incluyendo tableros dispuestos por el CSIRTAmericas. El propósito es reportar estas vulnerabilidades para un cierre diligente de brechas digitales y prevenir la materialización de riesgos e incidentes de seguridad que puedan afectar las operaciones. La identificación y corrección proactiva de vulnerabilidades asegurarán la disponibilidad e integridad de la información crítica.

ITEM	DESCRIPCIÓN
1.	El cooperante debe realizar el escaneo de vulnerabilidades en infraestructura crítica acorde con la definición del plan de trabajo entregado por el ColCERT.
2.	El cooperante debe realizar el monitoreo y evaluación de vulnerabilidades en tiempo real.
3.	El servicio debe realizar la revisión de protocolos de seguridad de correo electrónico (SPF, DKIM, DMARC).
4.	El servicio debe realizar la detección de sistemas obsoletos o sin parches en activos públicos.
5.	El servicio debe realizar la identificación de aplicaciones web expuestas con vulnerabilidades conocidas.
6.	El servicio debe realizar la evaluación de políticas de cifrado SSL/TLS en servicios web.
7.	El cooperante debe clasificar y priorizar vulnerabilidades según riesgo, criticidad y exposición.
8.	El cooperante debe monitorear la superficie de ataque digital de las entidades públicas, incluyendo dominios y subdominios de organizaciones
9.	El cooperante debe establecer un ciclo continuo de detección, análisis, remediación y validación de vulnerabilidades.
10.	El cooperante debe evaluar vulnerabilidades en aplicaciones web mediante pruebas automatizadas y manuales acorde con lo definido en plan de trabajo con el equipo ColCERT.
11.	El cooperante debe documentar procesos de gestión de vulnerabilidades y asegurar trazabilidad.
12.	El cooperante debe identificar patrones de riesgo comunes entre entidades para acciones preventivas sectoriales.
13.	El cooperante debe desarrollar y mantener dashboards en tiempo real del estado de vulnerabilidades.
14.	El cooperante debe realizar el escaneo de la superficie de ataque, identificando puntos de entrada vulnerables de las entidades públicas y privadas que se definan en el plan de trabajo mensual con el equipo ColCERT.
15.	El cooperante debe realizar revisiones periódicas para ajustar estrategias en conjunto con el ColCERT, según la evolución de las amenazas y tecnologías emergentes.

16.	El cooperante debe evaluar el riesgo asociado a cada vulnerabilidad identificada, teniendo en cuenta factores como el impacto y la probabilidad de explotación.
17.	El cooperante debe trabajar en conjunto con el ColCERT para abordar las vulnerabilidades que puedan ser explotadas en un ataque.

4.3 Línea de Servicio de transferencia de conocimiento y el acompañamiento en la Implementación de Lineamientos de la Política de Seguridad Digital

El cooperante destinará un recurso especializado por 12 meses para el diseño y la implementación de la estrategia de concientización y capacitación en ciberseguridad del ColCERT, dirigida a entidades públicas y privadas en Colombia. Este equipo se encargará de desarrollar presentaciones personalizadas, adaptadas a las necesidades específicas de cada entidad, con el propósito de promover una cultura robusta de seguridad digital entre funcionarios, contratistas y colaboradores.

El objetivo de esta estrategia incluye:

- **Concientizar** sobre la importancia de la ciberseguridad en el ámbito público y privado. Esto implica educar a los usuarios finales sobre las amenazas cibernéticas actuales y emergentes, así como sobre la relevancia de proteger la información y los sistemas críticos del gobierno y las empresas.

- **Sensibilizar** acerca de los riesgos y las consecuencias de los incidentes cibernéticos. Se busca que los participantes comprendan el impacto potencial de un ataque cibernético, no solo en términos de pérdida de datos, sino también en la interrupción de servicios esenciales y la afectación de la confianza pública.

- **Capacitar** en prácticas seguras y procedimientos establecidos para prevenir, detectar y responder a amenazas digitales. Esto incluye la formación en el uso de herramientas y tecnologías de seguridad, la implementación de políticas y procedimientos de ciberseguridad, y la preparación para la gestión de incidentes cibernéticos.

El equipo de trabajo dedicado a esta iniciativa estará compuesto por expertos en ciberseguridad con amplia experiencia en la creación de programas de capacitación efectivos. Además, se utilizarán metodologías de enseñanza innovadoras y recursos interactivos para asegurar que los participantes no solo adquieran conocimientos teóricos, sino que también desarrollen habilidades prácticas que puedan aplicar en sus roles diarios.

La estrategia de concientización y capacitación se llevará a cabo a través de una serie de talleres, seminarios y sesiones de formación, diseñados para ser accesibles y relevantes para todos los niveles de la organización. Se fomentará la participación y el intercambio de experiencias entre los asistentes, con el fin de crear una comunidad de práctica en

ciberseguridad que pueda colaborar y apoyarse mutuamente en la implementación de medidas de protección.

En resumen, esta iniciativa busca fortalecer la postura de ciberseguridad de las entidades públicas y privadas en Colombia, asegurando que todos los miembros de la organización estén equipados con el conocimiento y las herramientas necesarias para enfrentar los desafíos del entorno digital actual.

Frente al acompañamiento en la implementación de Lineamientos de la Política de Seguridad Digital se deben desarrollar como mínimo los siguientes aspectos:

ITEM	DESCRIPCIÓN
1.	El cooperante debe conformar un equipo consultor especializado a nivel de seguridad de la información, seguridad informática y ciberseguridad de modo que el equipo ColCERT cuente con apoyo para el despliegue implementación de Lineamientos de la Política de Seguridad Digital acorde con los requerimientos registrados en el ColCERT.
2.	El cooperante debe revisar, diseñar y desarrollar procedimientos para adopción de políticas en diferentes niveles de gobierno.
3.	El cooperante debe revisar, diseñar y proponer una metodología para la actualización periódica de políticas.
4.	El cooperante debe revisar, modificar/actualizar para establecer los requisitos mínimos de seguridad de la información, seguridad informática y ciberseguridad para proveedores y contratistas.
5.	El cooperante debe apoyar en el desarrollo normativo para desplegar la implementación de Lineamientos de la Política de Seguridad Digital a nivel público como privado y así mismo su registro en línea en el sitio que designe Mintic/ColCERT
6.	El cooperante debe generar paneles de visualización (dashboards) que muestren el estado de cumplimiento normativo de las entidades del orden nacional y territorial, utilizando las herramientas existentes en Mintic/ColCERT
7.	El cooperante debe incluir recomendaciones prácticas para cerrar brechas normativas detectadas durante el acompañamiento realizado.
8.	El cooperante a través del servicio de apoyo liderará mesas académicas para apoyar a las entidades pública sy oprivadas frente a la apropiación de Lineamientos de la Política de Seguridad Digital y acompañará a las entidades que así lo requieran en la aplicación de la misma.

4.4 Diseño, divulgación y despliegue catálogo de servicios del equipo ColCERT.

El cooperante deberá establecer un equipo especializado transversal encargado del diseño, elaboración y divulgación de materiales educativos y promocionales. Este equipo tendrá la responsabilidad entre otras generar contenidos como infografías, videos, reels y otros materiales gráficos. Su objetivo será facilitar el entendimiento y la adopción de conceptos

relacionados con soluciones de TI/OT, tipos de incidentes, herramientas, procesos, riesgos, vulnerabilidades, y la adopción de mejores prácticas y estándares, entre otros aspectos clave.

Este equipo trabajará en estrecha colaboración estrecha con el ColCERT para definir los entregables específicos que respondan tanto a las necesidades actuales como a los eventos coyunturales de seguridad digital que se desarrollen a nivel local, regional y global que puedan afectar a entidades públicas, privadas y a la ciudadanía en general. La coordinación efectiva asegurará que los contenidos producidos sean pertinentes y de alta relevancia. Las actividades de este equipo de diseño y divulgación se llevarán a cabo en modalidad 8/5 en las instalaciones designadas por el cooperante seleccionado. Este esquema operativo permitirá una dedicación efectiva durante el horario establecido, optimizando recursos y asegurando la entrega de materiales de alta calidad en tiempos definidos.

El cooperante deberá dimensionar el equipo de trabajo de acuerdo con el alcance de este servicio y tiempo empleado para su implementación.

8.2. Herramientas tecnológicas

El cooperante seleccionado debe asegurar que todas las soluciones, herramientas y plataformas proporcionadas estén debidamente licenciadas por el fabricante, por un periodo mínimo de doce (12) meses. Es fundamental que estas licencias incluyan actualizaciones a las versiones más recientes durante todo el período de vigencia del licenciamiento.

Así mismo debe realizar los ajustes y afinamiento inicial junto con el personal del ColCERT, garantizando el correcto funcionamiento de cada una de sus funcionalidades.

El soporte técnico debe ser realizado directamente por el fabricante, a cada una de las soluciones, herramientas y plataformas suministradas, el cual debe prestarse en la modalidad 7x24 para las herramientas y soluciones que requieren este servicio de soporte, para lo cual deberá entregar los respectivos protocolos de escalamiento de problemas.

8.2.1. Aspectos Clave del Licenciamiento y Soporte Técnico

- **Licenciamiento Completo**

Actualizaciones de Versiones: Las licencias deben incluir el derecho a recibir actualizaciones automáticas o versiones nuevas que se liberen para cada herramienta o plataforma, asegurando que el ColCERT siempre disponga de la tecnología más avanzada y segura.

Documentación de Licencias: El cooperante debe entregar toda la documentación relevante que certifique la autenticidad y la titularidad de las licencias para cada solución implementada.

- **Configuración y Afinamiento Inicial**

Colaboración con el ColCERT: El cooperante debe trabajar juntamente con el personal técnico del ColCERT para realizar la configuración inicial y el afinamiento de las soluciones, garantizando que todas las funcionalidades sean implementadas correctamente y optimizadas para el entorno específico del cliente.

Capacitación en Configuración: Además de la configuración inicial, el cooperante deberá proporcionar capacitación al personal del ColCERT para asegurar que puedan realizar ajustes y mantenimiento continuo eficazmente.

- **Soporte Técnico Directo del Fabricante**

Disponibilidad 7x24: El soporte técnico debe ser proporcionado directamente por el fabricante y estar disponible 24 horas al día, 7 días a la semana para aquellas herramientas y soluciones que soportan las verticales de análisis situacional, gestión de vulnerabilidades y gestión de incidentes, asegurando una respuesta rápida a cualquier incidencia crítica.

Protocolos de Escalamiento de Problemas: Deben establecerse y documentarse claramente los protocolos de escalamiento para problemas técnicos, facilitando una rápida resolución de incidencias y minimizando el impacto en las operaciones del ColCERT

- **Entrega de Documentación Contractual**

Documentos de Soporte y Mantenimiento: El cooperante seleccionado debe entregar al supervisor del contrato los documentos que acrediten los acuerdos de soporte y mantenimiento, incluyendo detalles de los niveles de servicio acordados (SLA), responsabilidades del fabricante, y cualquier otra obligación contractual relevante.
Transparencia y Cumplimiento: Esta documentación debe cumplir con todas las especificaciones técnicas y requerimientos legales, asegurando transparencia y conformidad con las regulaciones aplicables.

8.2.2. Renovación Herramientas

El cooperante debe renovar las siguientes herramientas por un periodo de doce (12) meses:

- **Mailchip (Standard) – Hasta 10.000 Correos electrónicos**

Una plataforma de automatización de marketing digital, enfocada en el envío masivo de correos electrónicos y campañas de email marketing directamente desde los buzones del

CSIRT Gobierno y ColCERT, se constituye como un canal estratégico para la difusión de comunicaciones esenciales. Esta herramienta permitirá la distribución eficiente de piezas informativas cruciales, tales como alertas tempranas, advertencias sobre amenazas, informes técnicos detallados y boletines informativos, emanados principalmente de la línea de análisis situacional. Al utilizar los canales de correo electrónico oficiales del CSIRT Gobierno y ColCERT, se asegura una mayor credibilidad y alcance de la información, facilitando que las entidades públicas y privadas en Colombia estén oportunamente informadas sobre el panorama de ciberseguridad y puedan tomar las acciones preventivas necesarias.

- **Cloudflare DNS**

El servicio de gestión y administración del Sistema de Nombres de Dominio (DNS) para colcert.gov.co reviste una importancia crítica para la correcta publicación y accesibilidad de los servicios del ColCERT en internet. Un DNS gestionado eficientemente garantiza que los usuarios puedan acceder sin problemas a la información, herramientas y recursos que el ColCERT ofrece. Esto implica la configuración precisa de los registros DNS, la monitorización constante para asegurar la resolución adecuada de nombres de dominio y la implementación de medidas de seguridad para proteger contra ataques como el DNS spoofing. En esencia, una administración robusta del DNS es fundamental para la presencia en línea confiable y la operatividad continua de los servicios del ColCERT.

- **Sistema Sandbox DoD**

La actualización del sistema Sandbox DoD a la última versión de Trellix Intelligent Sandbox representa un avance significativo para la capacidad del ColCERT de ofrecer servicios de análisis automatizado de malware. Esta modernización optimizará la detección y el análisis de amenazas sofisticadas, proporcionando información crucial a entidades públicas, privadas y a la ciudadanía en general. Adicionalmente, la migración del portal detectic.colcert.gov.co al portal web principal del ColCERT busca centralizar el acceso a este servicio, facilitando su adopción y uso. Esta integración no solo simplifica la interacción con la plataforma de sandbox, sino que también fortalece la oferta de servicios del ColCERT, consolidándolo como un referente en el análisis y la inteligencia de malware en Colombia. La continuidad de este servicio automatizado es fundamental para la respuesta proactiva ante incidentes de seguridad y para la mejora continua de la postura defensiva del país.

El desarrollo del Portal Conexión DoD se enfoca en establecer un canal de comunicación digital robusto y seguro para el intercambio de datos estructurados entre los sistemas relevantes, mediante la implementación de una API. Paralelamente, se construirá una interfaz gráfica intuitiva y de fácil acceso (front-end) que se integrará directamente en el sitio web del ColCERT. Esta integración garantizará una experiencia de usuario homogénea y consistente con la imagen institucional, al tiempo que cumple con los estándares técnicos y de seguridad definidos. El Portal detectic.colcert.gov.co facilitará la interacción y el acceso a funcionalidades específicas, optimizando los procesos y la colaboración dentro del entorno digital del ColCERT.

- **Kiteworks**

La continuidad de Kiteworks como herramienta de cifrado y descifrado de mensajes y archivos robustece significativamente la capacidad del CSIRT Gobierno y el ColCERT para compartir información sensible de manera segura con diversas entidades. Al integrar el cifrado directamente en el proceso de envío de correo electrónico a través de sus buzones oficiales (csirtgob@mintic.gov.co y contacto@colcert.gov.co), se garantiza la confidencialidad de los datos transmitidos. Kiteworks permite establecer un canal de comunicación protegido, asegurando que solo los destinatarios autorizados puedan acceder al contenido, mitigando así el riesgo de exposición de información crítica durante el intercambio. Esta funcionalidad es esencial para mantener la confianza y la seguridad en las comunicaciones del CSIRT Gobierno y el ColCERT con sus contrapartes en el sector público y privado.

- **Cisco Umbrella DNS Security Advantage**

Solución integral para fortalecer la seguridad de la red. Al operar a nivel del Sistema de Nombres de Dominio (DNS), esta herramienta intercepta y bloquea peticiones maliciosas antes de que se establezca una conexión, previniendo así el acceso a sitios web y contenidos peligrosos. Además de su función de bloqueo proactivo, Cisco Umbrella ofrece una valiosa visibilidad sobre la actividad DNS, permitiendo identificar patrones sospechosos y comprender mejor el panorama de amenazas. Su capacidad para extender la protección a usuarios remotos, independientemente de su ubicación, la convierte en un componente esencial para una estrategia de seguridad robusta y adaptable a las necesidades de las organizaciones modernas.

- **VMware ESXi, vCenter y vSphere**

El licenciamiento de VMware ESXi, vCenter y vSphere en su última versión es fundamental para optimizar el aprovechamiento de los recursos de procesamiento de los dos servidores Dell R660XSH2FY24v3. Estas soluciones de virtualización líderes en la industria permitirán consolidar cargas de trabajo, mejorar la eficiencia en la asignación de recursos, simplificar la administración del entorno de servidores y aumentar la disponibilidad de los servicios. Al implementar la última versión, el ColCERT se beneficiará de las funcionalidades más recientes en rendimiento, seguridad y gestión, asegurando una infraestructura virtualizada robusta y escalable para soportar sus operaciones críticas.

5. Actualización y Adquisición de herramientas y Software

Con el firme propósito de robustecer sus capacidades operativas y perfeccionar sus procesos internos, el ColCERT ha identificado la necesidad de actualizar y adquirir herramientas y software especializados en Detección y Respuesta Extendida. Esta inversión estratégica en tecnología tiene como objetivo primordial elevar la eficiencia, la seguridad y la calidad intrínseca de las linea de operación del ColCERT. Estas soluciones

tecnológicas son cruciales para dar respuesta a las exigencias actuales que demanda las amenazas, riesgos y vulnerabilidades de manera fundamental, La actualización y adquisición de estas herramientas no solo simplificará la gestión tanto en el ámbito técnico como en el administrativo, sino que también jugará un papel determinante en la mitigación de riesgos operativos y en la optimización del uso de los recursos disponibles, fortaleciendo así la capacidad del ColCERT para cumplir su misión de manera efectiva y segura.

8.3.3.1. Actualización e implementación Firewall de Nueva Generación

ITEM	DESCRIPCIÓN
1.	Cantidad dos (2) appliance de propósito especifico
2.	La solución de Firewall debe ser lideres en el cuadrante de Gartner
3.	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
4.	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
5.	Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación
6.	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7
7.	La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
8.	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP
9.	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding
10.	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM)
11.	Los dispositivos de protección de red deben soportar DHCP Relay
12.	Los dispositivos de protección de red deben soportar DHCP Server
13.	Los dispositivos de protección de red deben soportar sFlow
14.	Debe ser compatible con NAT dinámica (varios-a-1)
15.	Debe ser compatible con NAT dinámica (muchos-a-muchos)
16.	Debe soportar NAT estática (1-a-1)

17.	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces
18.	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
19.	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red
20.	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL
21.	Debe soporta protección contra la suplantación de identidad (anti-spoofing)
22.	Implementar la optimización del tráfico entre dos dispositivos
23.	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP)
24.	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales
25.	La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso
26.	Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos)
27.	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red
28.	• Debe soportar controles de zona de seguridad • Debe contar con políticas de control por puerto y protocolo • Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad • Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall • Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.

	• Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF) • Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes • Debe soportar el protocolo estándar de la industria VXLAN • La solución debe permitir la implementación sin asistencia de SD-WAN • En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN; • la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.
29.	Control de Aplicaciones • Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo • Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico • Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs • Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor • Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante • Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas; • Actualización de la base de firmas de la aplicación de forma automática • Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos • Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas • Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante

	• El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos; • Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo • Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video • Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo • Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) • Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación • Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación • Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
30.	Prevención de amenazas • Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo • Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware) • Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante; • Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad • Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos • Deber permitir el bloqueo de vulnerabilidades y exploits conocidos • Debe incluir la protección contra ataques de denegación de servicio • Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo • Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo • Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP; • Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP

	• Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets) • Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc • Detectar y bloquear los escaneos de puertos de origen • Bloquear ataques realizados por gusanos (worms) conocidos • Contar con firmas específicas para la mitigación de ataques DoS y DDoS • Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow) • Debe poder crear firmas personalizadas en la interfaz gráfica del producto; • Identificar y bloquear la comunicación con redes de bots; • Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo; • Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación; • Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos; • Los eventos deben identificar el país que origino la amenaza; • Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms); • Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP; • Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad; • En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles; • Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube)
31.	Filtrado URL • Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora) • Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración

	con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito • Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL • Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL • Tener por lo menos 75 categorías de URL • Debe tener la funcionalidad de exclusión de URLs por categoría • Permitir página de bloqueo personalizada • Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio) • Además del Explicit Web Proxy, soportar proxy web transparente;
32.	Identidad de Usuario • Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc • Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios • Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios • Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo) • Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios • Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD

	• Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma • Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores
33.	QoS • Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino • Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo • Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube • Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto • En QoS debe permitir la definición de tráfico con ancho de banda garantizado • En QoS debe permitir la definición de tráfico con máximo ancho de banda • En QoS debe permitir la definición de colas de prioridad • Soportar marcación de paquetes DiffServ, incluso por aplicación • Soportar la modificación de los valores de DSCP para Diffserv • Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service) • Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes
34.	DLP • Permite la creación de filtros para archivos y datos predefinidos • Los archivos deben ser identificados por tamaño y tipo • Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones • Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos • Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos • Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares

35.	Geo IP • Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países • Debe permitir la visualización de los países de origen y destino en los registros de acceso • Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas
36.	VPN • Soporte VPN de sitio-a-sitio y cliente-a-sitio • Soportar VPN IPSec • Soportar VPN SSL • La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512 • La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14 • La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2) • La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard) • Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall • Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec • Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting • Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy • Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL • Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local; • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL • Deberá mantener una conexión segura con el portal durante la sesión • El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
37.	FW Throughput 1 Gbps Concurrent Sessions (TCP): 700.000 New Sessions/Second (TCP): 35.000 IPsec VPN Throughput 6.5 Gbps IPS Throughput 1.4 Gbps Threat Protection Throughput 700 Mbps GE Interfaces: GE Interfaces: 5

8.3.3.2. Plataforma - eXtended Detection and Response - XDR

ITEM	DESCRIPCIÓN
1.	Se requiere la implementación de una plataforma XDR (eXtended Detection and Response) robusta y eficaz, capaz de detectar, contener y responder de manera integral ante amenazas avanzadas que puedan afectar los dispositivos finales de la organización, incluyendo servidores, equipos de escritorio (PCs) y entornos de infraestructura de escritorio virtual (VDI). Esta solución deberá tener la capacidad de cubrir un mínimo de quinientos (500) dispositivos, proporcionando una visibilidad unificada y una respuesta coordinada a través de las diferentes capas de seguridad, fortaleciendo así la postura defensiva del ColCERT contra ataques sofisticados y persistentes. Las licencias de la plataforma XDR deben ofrecer la flexibilidad de ser instaladas, desinstaladas y reinstaladas en diferentes entidades públicas y privadas dentro de Colombia, gestionadas de forma centralizada a través de una consola principal única. Esta característica es fundamental para permitir al ColCERT desplegar, administrar y reasignar la protección de XDR según las necesidades cambiantes de las diversas organizaciones a las que presta servicio, optimizando así el uso de las licencias y facilitando la supervisión y respuesta a incidentes de seguridad de manera unificada. La consola centralizada deberá proporcionar una visión completa del estado de seguridad de todos los dispositivos protegidos, independientemente de la entidad en la que se encuentren instalados.
2.	La plataforma debe ofrecer detección y respuesta en tiempo real a eventos maliciosos que ocurren en puntos finales, incluidos scripts maliciosos, ejecución PE anormal, malware sin archivos (fileless), exploits de aplicaciones y sistemas operativos, actividades de proceso anormales, scrapes de memoria y credenciales, shells inversos que tomen acciones maliciosas, exploits de día cero, ataques solo de memoria.
3.	La plataforma debe detectar acciones maliciosas en un equipo mediante técnicas de comportamiento (no basadas en firmas), y algoritmos de inteligencia artificial.
4.	La plataforma debe brindar protección contra ataques de día cero, mediante el análisis de comportamiento en el punto final, sin depender de firmas y reglas manuales.
5.	El agente debe incluir la creación de contexto de atributos en tiempo real de manera autónoma y automatizada, así como la correlación de eventos entre procesos.
6.	La plataforma ofrecida debe unificar y ampliar la capacidad de detección y respuesta a través de múltiples capas de seguridad. Debe incluir protección de endpoints (EPP), detección y respuesta de endpoints (EDR) en un solo agente para Windows, Mac, Linux, protección Kubernetes, S3, SDK y ambientes de almacenamiento como NETAPP

7.	La plataforma debe poder analizar eventos localmente en el agente sin dependencia de la nube.
8.	La plataforma no debe de tener dependencias de ciertos niveles de Kernel en Sistema Operativos de Linux.
9.	La plataforma no debe de depender de reinicio después de actualización del agente de protección o no debe de entrar en modo de protección reducida después de actualización de agente.
10.	La plataforma ofrecida debe proteger Workloads k8 de usuario final, en servidores y nativas de la nube
11.	Automatización a nivel de protección y respuesta sin depender de los datos históricos; debe proteger durante todo el ciclo de vida de la amenaza (pre-ejecución, ejecución, post-ejecución).
12.	Debe ser una plataforma de agente único, sin módulos adicionales, que se instalará en equipos, portátiles, servidores o máquinas virtuales, en sistemas operativos Windows, Linux y MacOS.
13.	Detectar y contener la ejecución de malware avanzado y malware de día 0 en el dispositivo final (PCs y Servidores). Debe ser basada en el análisis del comportamiento de la amenaza y su contexto en tiempo real sin el uso de reglas, firmas, conexión a la nube o sandbox.
14.	Debe tener la capacidad de remediar cambios al sistema operativo de manera automática usando la información aprendida por el agente de detección basado sobre el contexto de evolución de la amenaza para máquinas Windows y Mac
15.	Debe tener la capacidad de revertir cambios a archivos afectados durante un incidente en máquinas Windows (rollback) sin tener la necesidad de utilizar secuencia de comandos y debe ejecutarse manera automatizada, y/o con un solo con 1 solo click desde la consola en caso de ataques de ransomware. No debe de tener límite de numero de archivos o tamaño de archivos. Se debe de soportar archivos de 100 megas o más.
16.	La plataforma ofrecida debe permitir la conexión vía línea de comandos directamente desde la consola de administración a máquinas Windows, Mac, Linux y K8 con privilegios de sistema con una cuenta dinámica, que permita realizar investigación de ataques, recopilar datos forenses y remediar infracciones, sin importar dónde se encuentren los puntos finales comprometidos, eliminando la incertidumbre y reduciendo en gran medida cualquier tiempo de inactividad que resulte de un ataque
17.	La plataforma ofrecida debe proveer una característica que permita aislar un punto final de la red, excepto de la consola de administración, con propósito preventivo para detener la propagación de un incidente mientras se investiga una alerta. El aislamiento debe de tener la capacidad de agregar diferentes políticas de acceso en el caso que se necesite conectar el equipo a otros recursos.
18.	La plataforma debe contar con la opción para limitar la cantidad de agentes que pueden descargar una actualización en un momento dado.
19.	La plataforma debe contar con la opción de descargar el agente de una carpeta compartida dentro de la red durante actualización del agente.
20.	La plataforma ofrecida debe estar posicionada en el cuadrante de líderes de Gartner en los últimos tres años.

21.	La plataforma ofrecida debe participar en el análisis anual de MITRE ATT&CK para soluciones EDR y debe tener un cumplimiento mínimo del 99% en cada criterio de evaluación en los últimos 2 años.
22.	Debe permitir la detección, remediación y respuesta automatizada ante amenazas avanzadas, haciendo el mapeo de los indicadores de sistemas operativos Windows vigentes y Mac de amenazas con el framework de MITRE.
23.	Debe tener la capacidad de detección de amenazas avanzadas basado en Inteligencia artificial y por comportamiento localmente en el agente sin depender de reglas-preprogramadas.
24.	Debe permitir la creación de reportes que se puedan exportar desde la consola de administración.
25.	Debe permitir la visualización de todos los procesos/eventos que genera la detección.
26.	Debe contar con las funcionalidades de control de dispositivos (USB, Bluetooth y thunderbolt)
27.	Debe contar con la funcionalidad de control de firewall local.
28.	La plataforma debe brindar visibilidad de aplicaciones instaladas en los dispositivos finales indicando su nivel de riesgo y vulnerabilidades asociadas.
29.	La plataforma debe unificar las funciones de prevención y detección de dispositivos, detección de puntos finales y rendición de cuentas sin depender de datos históricos, y debe realizar funciones de detección y ejecución automáticas, búsqueda de incidentes de seguridad en una única solución.
30.	Los agentes de la solución ofrecida deben ser resistentes a la manipulación y tener una lógica local de prevención, detección y respuesta para que el propio agente reduzca significativamente la duración de la permanencia del ataque.
31.	Debe guardar 365 días de historial de datos de incidentes almacenados directamente en la consola en la nube.
32.	El agente debe ser autónomo, realizar detección y mitigación en tiempo real sin la ayuda o intervención de un Centro de Operaciones de Seguridad (SOC).
33.	La plataforma debe correlacionar los eventos del endpoint en una línea de tiempo que permita encontrar de manera rápida todos los procesos, archivos, subprocesos, eventos y otros datos relacionados en una sola consulta, permitiendo identificar la causa raíz.
34.	La plataforma permite buscar desde la consola Indicadores de compromiso (IoC) como (procesos, comandos, powershell, CMD, hash, extensión de archivos)
35.	La plataforma debe proveer retención de logs de EDR por 14 días como mínimo sin costo adicional, con capacidad de retención de logs hasta 2 años.
36.	Debe permitir la creación de consultas personalizadas para cacería de amenazas (threat hunting).
37.	Debe permitir realizar consultas de IOC de manera masiva.

38.	Debe tener la capacidad de guardar las consultas de búsqueda como reglas personalizadas y aprovecharlas para crear alertas contra eventos en tiempo real y responder automáticamente a las amenazas
Plataforma	
39.	La plataforma debe clasificarse como ACTIVE EDR – XDR.
40.	Debe tener la consola de administración 100 % en la nube.
41.	Debe ser una consola multiusuario, multisitio y multigrupo que permita la creación de usuarios con independencia y accesos con diferentes roles.
42.	La consola de administración debe implementar la API RESTful o equivalente para fines de integración con herramientas de cualquier sistema que admita la integración de API.
43.	La autenticación en la plataforma puede realizarse haciendo SSO y habilitando un segundo factor de autenticación para validar otro parámetro y confirmar la petición del usuario.
44.	La plataforma debe controlar los "grupos dinámicos" en función de etiquetas (TAGS) u otros atributos. Asegurando de que esté disponible en todas las superficies, incluidas: Windows, macOS, Linux, K8s, etc
45.	Debe incluir un catálogo de exclusiones (mínimo 78 aplicaciones) para los procesos corriendo en los sistemas operativos en Windows, macOS, Linux y contenedores.
46.	La auditoría y el registro de actividad deben mantenerse en la consola de administración
47.	La plataforma a ofertar debe tener una base de conocimiento y documentación dentro de la consola sin la necesidad de utilizar credenciales de otro sistema.
48.	La solución debe tener una plataforma avanzada que centralice datos de tu entorno y de seguridad, facilitando la detección temprana y la respuesta rápida a amenazas al consolidar datos EDR, XDR y de terceros en una sola consola unificada.
49.	Debe tener la capacidad de extraer datos no estructurados de terceros en la plataforma y correlacionarlos con cualquier evento existente en la plataforma EPP/EDR.
50.	Debe de incluir por lo menos 10 gigas de datos al día sin costo con la capacidad de extender hasta 2 años.
51.	La plataforma debe poder tener la capacidad de aumentar su ingesta de datos hasta 20 terabytes de datos por día y permanecer en un estado de funcionamiento estable.
52.	Debe tener la capacidad de ejecutar consultas complejas en al menos 1 TB de datos y devolver resultados en menos de un minuto.
53.	Debe tener la capacidad de visualizar datos de terceros junto con los datos de seguridad de la plataforma nativa.
54.	La plataforma debe permitir hacer integraciones con soluciones de seguridad de terceros a través de su Marketplace que sea simple de configurar y administrar.
55.	Debe de tener la capacidad de analizar consultas completas de todos los datos ingeridos y datos generados por los agentes

56.	La plataforma debe poder ingerir terabytes/petabytes de datos por día y permanecer en un estado de funcionamiento estable.
57.	La Plataforma, permitir eel despliegue en los siguientes sistemas operativos: Debe soportar: • Windows XP SP3 or later 32/64-bit • Windows 7 SP1, 8, 8.1, 10, 11 • Windows Storage Server 2012, 2012 R2, 2016 • Windows Server 2003 SP2, W 2003 R2 SP2 , 32/64-bit , 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022. • MacOs: Ventura, Monterey, Big Sur • CentOS: 6.4+, 7.0-7.8, 7.9, 8.0, 8.1. 8.2, 8.3, 8.4 • RedHat Enterprise Linux: 6.4+, 7.0 - 7.8, 7.9, 8.0 – 8.3 - 8.4 – 8.6, 8.7, 9.0 • Ubuntu: 14.04, 16.04, 18.04, 19.04, 19.10, 20.04 -22.04 • Amazon: 2017.03, 2018.03, AMI 2 • SUSE Linux Enterprise Server: 12.x, 15.x • Debian: 8,9,10, 11 • Virtuozzo: 7 • Scientific Linux: 6,7 • AlmaLinux: 8.4, 8.5, 8.6, 8.7, 9.0 • RockyLinux: 8.4, 8.5, 8.7, 9.0 • Linux Distro: 6.9,6.10 – 7.0 -7.8, 7.9 8.0 – 8.3, 8.4 • Oracle: 6.9, 6.10, 7.0 - 7.9, 8.0 - 8.5, 8.6, 8.7, 9.0 • Fedora: 15-30, 31, 33, 32, 34, 35, 36

6. ENTRENAMIENTO EN USO DE HERRAMIENTAS

Con el objetivo primordial de asegurar la correcta operación y el máximo aprovechamiento de las funcionalidades inherentes a cada una de las herramientas y soluciones renovadas, adquiridas y entregadas por el proveedor, se establece la obligatoriedad de desarrollar un cronograma detallado para la transferencia de conocimiento. Este cronograma deberá contemplar sesiones de capacitación exhaustivas dirigidas a los analistas de seguridad del Equipo ColCERT, abordando aspectos cruciales como la instalación, la implementación y la operación de cada nueva solución. Se estipula un mínimo de diez (10) horas de instrucción para cada herramienta nueva, asegurando una comprensión profunda de sus capacidades.

De manera similar, para las herramientas que hayan sido renovadas y actualizadas, se requerirá un cronograma específico para la actualización de conocimientos sobre las nuevas funcionalidades incorporadas. Estas sesiones de actualización para los analistas de seguridad del Equipo ColCERT deberán tener una duración mínima de cuatro (4) horas por cada solución renovada, garantizando que el equipo esté al tanto de las últimas mejoras y características.

El proveedor deberá asegurar que la transferencia de conocimiento para cada una de las herramientas tecnológicas detalladas en el Anexo Técnico sea impartida por personal técnico altamente especializado, que cuente con certificaciones vigentes emitidas por el fabricante o por un organismo de certificación internacional reconocido en relación con dichas herramientas. Además, este personal deberá acreditar una experiencia mínima de dos (2) años en la implementación de la herramienta específica objeto del contrato.

Es igualmente mandatorio que esta transferencia de conocimiento se extienda a cada nuevo analista de seguridad que se integre al Equipo ColCERT durante el periodo de vigencia del licenciamiento, soporte y mantenimiento de las soluciones. Esto asegura una capacitación continua y la rápida integración de nuevos miembros al equipo.

La planificación y ejecución de la transferencia de conocimiento deberán considerar todas las soluciones, herramientas y plataformas licenciadas y entregadas para la óptima operación del Equipo ColCERT, garantizando una capacitación integral y adaptada a las necesidades específicas de cada tecnología implementada.

8.3. Capacitación Presencial

Se requieren tres (3) sesiones de 2 horas cada una, para la transferencia de conocimiento a los analistas de seguridad del Equipo ColCERT que realizarán la operación de las herramientas y soluciones, dichas capacitaciones se centrarán en aspectos funcionales, de configuración y de operación de las soluciones, herramientas y plataformas.

8.4. Capacitación Virtual

La metodología de transferencia de conocimiento virtual contempla (2) dos sesiones de 2 horas cada una, a través de la plataforma Teams de la entidad designada por la Corporación, para los analistas de seguridad del Equipo ColCERT.

9. LICENCIAMIENTO Y SOPORTE TÉCNICO

Es un requisito indispensable que todas las soluciones, herramientas y plataformas renovadas y suministradas por el proveedor cuenten con las licencias correspondientes emitidas directamente por el fabricante. Estas licencias deberán incluir el derecho a recibir todas las actualizaciones y nuevas versiones que se liberen para cada uno de los productos durante la totalidad del periodo de vigencia tanto del licenciamiento como del servicio contratado. Esta condición asegura que el ColCERT siempre disponga de las últimas funcionalidades, mejoras de seguridad y parches disponibles, manteniendo así la infraestructura tecnológica actualizada y optimizada a lo largo del tiempo.

Para garantizar la continuidad operativa y la resolución eficiente de cualquier eventualidad, se requerirá que el soporte técnico y el mantenimiento de cada una de las soluciones, herramientas y plataformas renovadas y suministradas sean proporcionados

directamente por el fabricante. Este soporte deberá ofrecerse bajo la modalidad 5x8 (cinco días a la semana, ocho horas al día). En este sentido, el proveedor tendrá la responsabilidad de entregar al ColCERT los protocolos detallados de escalamiento de problemas, especificando los niveles de soporte, los tiempos de respuesta esperados para cada nivel y los procedimientos a seguir en caso de requerir una atención más especializada por parte del fabricante. Estos protocolos son esenciales para asegurar una gestión ágil y efectiva de cualquier incidente técnico que pueda surgir.

El proveedor deberá entregar al supervisor del contrato toda la documentación técnica necesaria para la correcta implementación, operación y mantenimiento de las soluciones adquiridas. Esta información deberá incluir, pero no limitarse a, manuales de usuario detallados que permitan al personal del ColCERT utilizar eficientemente las herramientas y software. Asimismo, se deberán entregar manuales de administración y configuración que faciliten la gestión y personalización de los sistemas. Es crucial que la documentación técnica sea clara, concisa, esté en idioma español y contemple todos los aspectos relevantes para garantizar la autonomía y el aprovechamiento óptimo de la inversión tecnológica realizada por el ColCERT.

Adicionalmente a la documentación técnica, el proveedor estará obligado a entregar al supervisor del contrato los soportes legales y contractuales correspondientes a cada una de las soluciones, herramientas y plataformas suministradas. Esto incluye las licencias de software con sus respectivos términos y condiciones de uso, así como los contratos de soporte técnico y mantenimiento que garanticen la continuidad operativa y las actualizaciones necesarias para cada uno de los elementos adquiridos. Estos documentos deberán detallar los niveles de servicio (SLAs), los tiempos de respuesta, los mecanismos de escalación y la vigencia de los servicios de soporte y mantenimiento, asegurando así la protección de la inversión del ColCERT y la disponibilidad de asistencia especializada cuando sea requerida, todo ello en estricta conformidad con las especificaciones técnicas establecidas en el contrato.

El proveedor será responsable de llevar a cabo la configuración y el afinamiento inicial de las herramientas adquiridas y las soluciones renovadas, trabajando en estrecha colaboración con el equipo técnico del ColCERT. Este proceso conjunto asegurará la correcta implementación de todas las funcionalidades ofrecidas, permitiendo al personal del ColCERT adquirir el conocimiento práctico necesario para la administración y el uso eficiente de las nuevas tecnologías. La participación activa del equipo del ColCERT en esta etapa de configuración y afinamiento es crucial para garantizar que las soluciones se adapten a las necesidades específicas de las entidades y para facilitar una transición fluida hacia su operación autónoma.

Nota 1: El plazo para la entrega de las herramientas tecnológicas incluyendo su licenciamiento será máximo dentro de los treinta (30) días calendario siguientes a la suscripción del Acta de Inicio.

Nota 2: El soporte técnico será de doce (12) meses. contado a partir del recibo de las herramientas tecnológicas y su licenciamiento.

10. ACUERDOS DE NIVELES DE SERVICIO – ANS

Disponibilidad de las herramientas:

La disponibilidad se medirá usando la siguiente ecuación:

$$\left(1 - \frac{Número\ total\ de\ minutos\ que\ la\ herramienta\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ x24\ horas\ x60\ minutos}\right) x100\%$$

La indisponibilidad es el número total de minutos, durante el mes, en los que la herramienta no está disponible, dividido en el número total de minutos en el mes.

La medición se hace de manera independiente para cada una de las herramientas, para lo cual el proveedor realizara el monitoreando permanentemente a cada uno de ellos durante el mes. Los resultados del monitoreo son mantenidos por el proveedor para que puedan ser consultados por Equipo ColCERT en cualquier momento durante la ejecución del contrato. La información mantenida por el proveedor le debe permitir al ColCERT, verificar la disponibilidad histórica en los meses anteriores y durante el mes en curso.

La medición se hace de forma individual sobre cada herramienta contratada. Es decir, cada herramienta debe cumplir con el valor exigido en el ANS.

ANS	
Disponibilidad exigida herramientas >=99.99% mensual	

Interrupciones

Hace referencia a el número máximo de Interrupciones durante el mes.

Una Interrupción se define como una pérdida total de la operación de la herramienta que implica que no hay operación.

La medición la hace el proveedor monitoreando permanentemente durante el mes las herramientas. Los resultados del monitoreo son mantenidos por el proveedor para que puedan ser consultados por el Equipo ColCERT en cualquier momento durante la ejecución del contrato. La información mantenida por el proveedor le debe permitir Al Equipo ColCERT verificar el número de Interrupciones histórico de meses anteriores y el número de Interrupciones acumuladas para el mes en curso.

<table>
<tr><td colspan="2">La medición se hace de forma individual sobre cada herramienta. Es decir, cada herramienta debe cumplir con el valor exigido en el ANS</td></tr>
<tr><td>ANS</td><td></td></tr>
<tr><td>Interrupciones máximas en un mes:</td><td>2 interrupciones</td></tr>
<tr><td colspan="2">Efectividad en resolución de incidentes/solicitudes:</td></tr>
<tr><td colspan="2">Mide el nivel de cumplimiento del total de solicitudes recibidas en un periodo de un me

por los canales de atención definidos y penaliza cuando la efectividad en la atención

supera el ANS definido.

El Proveedor debe contar con una mesa de ayuda 5x8 según sea el caso, para las herramientas y soluciones que requieren este servicio de soporte, que le permita al Equipo ColCERT reportar cualquier requerimiento y problema presentando con cada una de las herramientas y servicios contratados.

La efectividad de resolución de solicitudes mide el tiempo máximo de solución de las solicitudes realizadas a la mesa de ayuda del proveedor según su nivel de prioridad.

El reloj que mide la efectividad de resolución comienza a contabilizar el tiempo desde el momento en que el ticket es registrado en la mesa de ayuda hasta que el proveedor da una respuesta y soluciona el problema Nivel de Escalabilidad, el proveedor debe entregar un documento donde se especifique los niveles de escalabilidad de requerimientos, el cual debe contener entre otros, números telefónicos de contacto de la mesa de servicio, líder del proyecto, árbol telefónico comercial, técnico, soporte nivel 1,2 y 3

La efectividad en la atención se mide usando la siguiente fórmula:

Solicitudes (Llamadas, chat, registros o email) atendidas dentro del tiempo definid
---------- X 100
Total de Solicitudes recibidas (Llamadas, chat, registros o email)</td></tr>
<tr><td>ANS</td><td>Tiempo</td></tr>
</table>

Efectividad en la atención >= 90% no conformidad = 100 – ANS	Prioridad 1: Efectividad de resolución <=2 horas Prioridad 2: Efectividad de resolución <= 4 horas Prioridad 3: Efectividad de resolución <= 8 horas

11. SEGURIDAD DE LA INFORMACION.

El proveedor deberá tener implementado un modelo de seguridad de la información y alienar sus procesos y procedimientos internos relacionados con la ejecución del presente proyecto, acorde con lo definido en lo referente a Seguridad y Privacidad de la Información por parte de la entidad designada por la Corporación, teniendo en cuenta lo definido en los numerales del presente capítulo.

Se debe mantener la confidencialidad de la información propiedad de la entidad a que tenga acceso en el marco de ejecución del contrato, así mismo cuando termine el contrato deberá entregar a la entidad toda la información que este solicite garantizando que la misma es propiedad de la entidad. El proveedor se compromete a no divulgar la información obtenida durante la ejecución del contrato a terceras personas.

El personal técnico y profesional especializado del proveedor a cargo del proyecto, implementación, despliegue, soporte y mantenimiento, deberá firmar un acuerdo de confidencialidad, para garantizar la reserva de la información del ColCERT a la cual tengan acceso

12. CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE PROTECCIÓN DE DATOS DEL MINTIC

El proveedor deberá alienar sus procesos, procedimientos y formatos internos relacionados con la ejecución del presente proyecto, a los estándares que actualmente maneje la entidad designada por la Corporación.

Se debe mantener la confidencialidad, integridad y disponibilidad de la información, propiedades de la entidad a que tenga acceso en el marco de ejecución del contrato, así mismo cuando termine el contrato deberá entregar a la entidad toda la información que este solicite garantizando que la misma es propiedad de la entidad. El proveedor se compromete a no divulgar la información obtenida durante la ejecución del contrato a terceras personas.

El personal técnico y profesional especializado del proveedor a cargo del proyecto, implementación, despliegue, soporte y mantenimiento, deberá firmar un Acuerdo de

confidencialidad, Autorización de tratamiento de Datos, Conflicto de Intereses y demás documentos, para garantizar la reserva de la información del GIT de del Respuesta a Emergencias Cibernéticas de Colombia - ColCERT a la cual tengan acceso.

Siendo así, el proveedor se debe alinear y cumplir lo establecido en el Sistema de Gestión de Seguridad y Privacidad de la información que viene implementando la entidad designada por la Corporación, y dar cumplimiento a la Resolución No 2239 del 2024, la cual actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad y Continuidad de la Operación de los servicios de la entidad designada por la Corporación, la cual establece en el su Artículo 2 Ámbito de aplicación:

"Política General de Seguridad y Privacidad de la Información, Seguridad y Continuidad de la Operación de los servicios del Ministerio/Fondo único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de las Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen intercambien o consulten su información, al igual que a las entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información independiente de su ubicación. De igual manera, esta política aplica a toda información creada, procesada o utilizada por el Ministerio/Fondo único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre."

Resolución 2239 de 2024.

Así mismo, la Política de Seguridad y Privacidad de Información de la entidad designada por la Corporación se implementa por medio de manuales, procedimientos, formatos, compromisos de confidencialidad, etc. Los cuales el proveedor deberá dar cumplimiento durante su vinculación con la entidad.

Finalmente, en línea con la política de protección de datos personales de la entidad designada por la Corporación. La Resolución 2238 del 2024, el contratista debe garantizar el cumplimiento de los dispuesto en dicha resolución.

Resolución 2238 de 2024