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)*

- **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)*

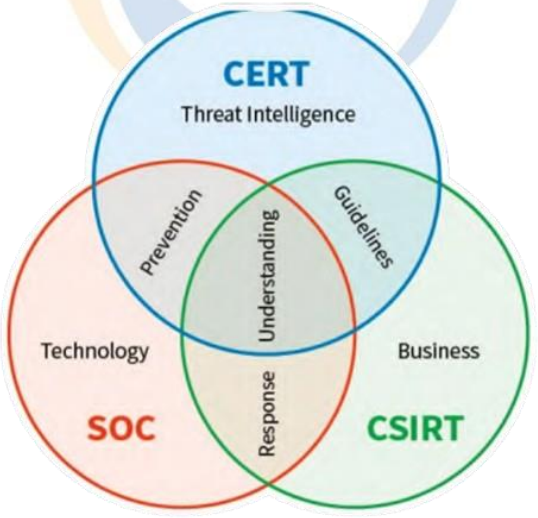

Figura 1: Relación CERT/CSIRT/SOC
Fuente: Exabeam

TIPOS DE SOC

- **1. SOC Privados:** Los **SOC Privados** son centros de operaciones de ciberseguridad que funcionan dentro del sector privado. Su objetivo principal es proteger la infraestructura y los datos de la empresa contra ciberamenazas. Estos SOC son responsables de la monitorización continua de los sistemas y redes de la organización, la detección de incidentes, la respuesta a amenazas y la gestión de la seguridad en un entorno empresarial específico. *(ISACA. (2020). "Cybersecurity Practices: A Guide for Your Organization". ISACA Journal. ISACA Cybersecurity Practices)*

- **2. SOC Sectoriales:** Los **SOC Sectoriales** son centros de operaciones de ciberseguridad diseñados para abordar las necesidades de seguridad de un sector específico. Por ejemplo, pueden estar enfocados en la salud, finanzas, educación, o cualquier otro sector crítico. Estos SOC cuentan con experiencia y conocimiento especializados en las amenazas y vulnerabilidades particulares que enfrenta su sector, permitiendo una respuesta más efectiva y adaptada a las características del mismo. *(ENISA. (2020). "Sectoral Approach to Cybersecurity". European Union Agency for Cybersecurity. ENISA Sectoral Approach)*

- **3. SOC de Entidades Locales:** Los **SOC de Entidades Locales** son centros de ciberseguridad que operan a nivel de gobiernos locales o regionales. Su función es proteger los sistemas y servicios públicos de las entidades gubernamentales en una determinada localidad. Esto incluye la detección y respuesta a incidentes de seguridad que puedan afectar a la administración pública y a los ciudadanos. Este tipo de SOC es crucial para mantener la confianza pública en los servicios gubernamentales. *(National Cyber Security Centre (NCSC). (2018). "Local Government Cyber Security". NCSC Guidance.* NCSC Local Government Cyber Security*)*

- **4. SOC Ministeriales:** Los **SOC Ministeriales** son centros de operaciones de ciberseguridad que se ocupan de la protección de las infraestructuras digitales y de la información en los ministerios y otras entidades gubernamentales. Su enfoque es garantizar la seguridad de los datos sensibles y la continuidad operativa de los servicios que proporcionan. Estos SOC trabajan en coordinación con otros organismos gubernamentales para abordar las amenazas a la ciberseguridad a nivel nacional. *(Federal Bureau of Investigation (FBI). (2021). "Cybersecurity for Government Agencies". FBI Guidance. FBI Cybersecurity for Government)*

- **5. SOC Nacional (Centro de Operaciones de Ciberseguridad) de la Administración General del Estado:** El **SOC Nacional** es un centro nacional que coordina y supervisa la ciberseguridad en el ámbito de la Administración General del Estado. Su labor incluye la gestión de incidentes de seguridad que puedan afectar a las instituciones gubernamentales, la coordinación de la respuesta a ciberamenazas y la promoción de políticas de ciberseguridad en todo el gobierno. El COCS actúa como un ente regulador y colaborativo entre los diferentes SOC y CERT en el país. *(Gobierno de España. (2020). "Plan Nacional de Ciberseguridad". Ministerio de Asuntos Económicos y Transformación Digital. Plan Nacional de Ciberseguridad)*

Al considerar la capacidad instalada de un SOC Nacional, es importante evaluar:

- La infraestructura tecnológica disponible y su escalabilidad.
- La experiencia y certificaciones del personal que operará el SOC.
- Los procesos y protocolos establecidos para la gestión de incidentes.

- La integración con otros equipos como CERT y CSIRT.
- Las capacidades de análisis de datos y respuesta automatizada.

CONTEXTO TÉCNICO

En la actualidad, la ciberseguridad se ha convertido en una prioridad fundamental para los gobiernos y las organizaciones en todo el mundo. La creciente sofisticación de las amenazas cibernéticas exige la implementación de estrategias y estructuras robustas para proteger la infraestructura crítica y los datos sensibles. Dentro de este contexto, surgen tres conceptos clave: el **CERT Nacional**, el **CSIRT de Gobierno** y el **SOC (Security Operations Center)**, cada uno desempeñando un papel crucial en la defensa cibernética.

El **CERT Nacional** actúa como un punto focal de respuesta a incidentes de seguridad digital a nivel nacional. Su misión es coordinar y gestionar la respuesta ante incidentes cibernéticos, proporcionando asistencia técnica y directrices a las entidades gubernamentales y al sector privado. Este equipo fomenta la colaboración y el intercambio de información sobre amenazas, contribuyendo a mejorar la resiliencia cibernética del país.

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** es una unidad centralizada dedicada a la monitorización continua y la gestión de incidentes de seguridad. Equipado con tecnología avanzada, como sistemas de gestión de información y eventos de seguridad (SIEM), el SOC es responsable de la detección y respuesta a amenazas en tiempo real, garantizando que las organizaciones puedan reaccionar de manera rápida y efectiva ante incidentes cibernéticos.

En conjunto, la interacción entre las la entidades designadas por la Corporación Colombia Digital y el SOC constituye una defensa integral contra las amenazas cibernéticas, permitiendo una gestión eficaz de la seguridad en el entorno digital. La adecuada contratación y desarrollo de la capacidad instalada de un SOC Nacional es, por tanto, esencial para fortalecer la postura de ciberseguridad del país y garantizar la protección de sus infraestructuras críticas y servicios esenciales.

JUSTIFICACIÓN TÉCNICA

El entorno de ciberseguridad en Colombia ha enfrentado desafíos significativos en los últimos años, con un aumento en la frecuencia y sofisticación de los ataques dirigidos a infraestructuras críticas. Estos ataques no solo comprometen la seguridad de la información, sino que también representan un riesgo considerable para la continuidad operativa de servicios esenciales que sostienen la vida

económica y social del país. En respuesta a esta situación, La entidad designada por la Corporación Colombia Digital ha desempeñado un rol vital, pero su capacidad operativa debe ser fortalecida mediante la adquisición de herramientas tecnológicas avanzadas con un enfoque en ciberseguridad.

En 2023 y 2024, Colombia ha sido testigo de varios ataques cibernéticos significativos que han puesto en riesgo la seguridad de sus infraestructuras críticas. Entre los incidentes más relevantes, destacan los ataques dirigidos a sectores como la energía, las telecomunicaciones y la banca. En 2023, un ataque masivo de ransomware afectó a una de las principales empresas de energía del país, lo que resultó en una interrupción temporal de los servicios de distribución eléctrica en varias regiones. Este incidente no solo comprometió la operatividad de la empresa afectada, sino que también puso en evidencia las vulnerabilidades en la protección de infraestructuras críticas frente a ataques cibernéticos.

En 2024, otro ataque significativo fue el que afectó al sector financiero, donde una serie de ataques de phishing y de denegación de servicio (DDoS) comprometieron la seguridad de varias entidades bancarias, interrumpiendo temporalmente las transacciones y generando pérdidas económicas millonarias. Estos incidentes subrayan la urgencia de fortalecer las capacidades de respuesta de la entidad designada por la Corporación Colombia Digital para proteger la estabilidad económica y social del país frente a amenazas cibernéticas.

Este proceso se construye con base a la necesidad de implementar un proyecto que dote a la entidad designada por la Corporación Colombia Digital de capacidades avanzadas en gestión del gobierno, control de la superficie de ataque, ciberinteligencia, ciberinvestigación, monitorización de información crítica y entrenamiento especializado. La mejora de estas áreas permitirá a la entidad designada por la Corporación Colombia Digital no solo responder de manera más efectiva a las amenazas actuales, sino también anticiparse a las nuevas vulnerabilidades emergentes en el ciberespacio.

Las amenazas cibernéticas no solo han aumentado en número, sino que también han evolucionado en complejidad, con el uso de inteligencia artificial (IA) por parte de actores maliciosos para desarrollar ataques más sofisticados y difíciles de detectar. La IA se ha convertido en una herramienta poderosa en manos de cibercriminales, que la utilizan para automatizar ataques de phishing, diseñar malware más evasivo y realizar ataques de ingeniería social más persuasivos.

En 2024 también se reportaron incidentes donde los atacantes utilizaron IA para generar deepfakes altamente convincentes, que fueron empleados para engañar a ejecutivos y obtener acceso no autorizado a sistemas críticos. Además, los ataques con IA pueden adaptarse en tiempo real a las defensas implementadas por las organizaciones, lo que hace que las estrategias tradicionales de ciberseguridad sean insuficientes para protegerse contra estas nuevas amenazas.

En este contexto, es imperativo que a la entidad designada por la Corporación Colombia Digital cuente con servicios tecnológicos avanzados que incluyan capacidades de ciberinteligencia basadas en IA, para detectar y neutralizar estas amenazas antes de que causen daños significativos.

Contar con estas capacidades en el portafolio permitirá a la entidad designada por la Corporación Colombia Digital mantenerse a la vanguardia en la defensa cibernética, anticipando las tácticas de los atacantes y protegiendo de manera proactiva las infraestructuras críticas del país.

La capacidad de respuesta y recuperación ante incidentes cibernéticos es un aspecto crucial para la resiliencia de las infraestructuras críticas. Un enfoque robusto en la gestión del gobierno dentro de la entidad designada por la Corporación Colombia Digital es esencial para garantizar que los protocolos de respuesta a incidentes sean efectivos y se puedan ejecutar sin contratiempos. Esto incluye la implementación de un Protocolo de Recuperación de Desastres (DRP) que cubra todos los servicios ofrecidos por la entidad designada por la Corporación Colombia Digital, asegurando que cualquier interrupción causada por un ataque cibernético sea gestionada de manera eficiente y que las operaciones normales se restablezcan en el menor tiempo posible.

Además, la implementación de servicio de sistema de control de superficie de ataque permitirá a la entidad designada por la Corporación Colombia Digital identificar rápidamente las áreas más vulnerables en las infraestructuras críticas y actuar de manera preventiva. Este control es fundamental para minimizar el impacto de los ataques y garantizar que las infraestructuras críticas puedan continuar operando incluso bajo condiciones adversas.

La adquisición de un servicio de entrenamiento para los equipos Red y Blue dentro de la entidad designada por la Corporación Colombia Digital es fundamental para asegurar que el personal esté preparado para enfrentar ataques en escenarios reales. La formación constante en un entorno controlado permitirá al equipo mejorar sus habilidades tanto en ataque como en defensa, asegurando una respuesta ágil y efectiva ante cualquier amenaza que pueda surgir.

Los antecedentes recientes de ataques cibernéticos en Colombia, combinados con la aparición de nuevas amenazas potenciadas por IA, subrayan la importancia de dotar a la entidad designada por la Corporación Colombia Digital de servicios avanzados que permitan una gestión eficaz del gobierno, un control riguroso de la superficie de ataque, una ciberinteligencia proactiva, y una ciberinvestigación exhaustiva.

Asimismo, mejorar las capacidades de monitorización de información crítica y asegurar un entrenamiento continuo para los equipos de ciberseguridad es vital para garantizar la resiliencia de las infraestructuras críticas del país. Este proceso no solo permitirá a la entidad designada por la Corporación Colombia Digital fortalecer sus capacidades de respuesta, sino que también posicionará a Colombia como un referente en ciberseguridad a nivel regional e internacional, protegiendo de manera efectiva el ciberespacio nacional frente a las amenazas actuales y futuras.

GENERALIDADES

OBJETIVOS

Objetivo General

Fortalecer las capacidades operativas y estratégicas de la entidad designada por la Corporación Colombia Digital mediante la implementación de componentes esenciales tecnológicamente avanzados enfocados en ciberseguridad orientados a la disposición de la capacidad instalada del Centro de Operaciones de Seguridad – SOC Nacional, con el fin de proteger las infraestructuras críticas de Colombia, mejorar la respuesta a incidentes cibernéticos y anticiparse a las amenazas emergentes.

Objetivos Específicos

1. Establecer una gestión del gobierno dentro del la entidad designada por la Corporación Colombia Digital, que incluya el servicio de la gestión de gobierno, así como un Protocolo de Recuperación de Desastres (DRP) que abarque todos los servicios ofrecidos.
2. Implementar un Servicio de sistema de control de superficie de ataque que permita identificar y monitorizar en tiempo real las vulnerabilidades y la exposición a riesgos cibernéticos de las entidades que consultan y consumen los servicios de seguridad de la entidad designada por la Corporación Colombia Digital.
3. Implementar un servicio de ciberinteligencia que facilite la identificación, evaluación y gestión de la huella digital de las entidades, así como la determinación del score de riesgo asociado a sus identidades digitales.
4. Poner en marcha servicio de ciberinvestigación global que permita a la entidad designada por la Corporación Colombia Digital realizar investigaciones detalladas sobre incidentes cibernéticos, interpretando objetos asociados y compartiendo de manera segura objetos de seguridad con otras entidades.
5. Implementar servicio de monitorización de información crítica que permita el seguimiento y control de documentos sensibles, garantizando que solo personal autorizado tenga acceso a esta información, y asegurando la protección de datos de alta criticidad.
6. Dotar a la entidad designada por la Corporación Colombia Digital con servicio de entrenamiento para los equipos Red y Blue, mejorando sus capacidades de ataque y defensa mediante la simulación de escenarios reales de ciberataques, con el fin de mantener a los equipos capacitados y preparados para enfrentar las amenazas cibernéticas.

ALCANCE

La implementación de un SOC Nacional para la entidad designada por la Corporación Colombia Digital tiene como objetivo principal fortalecer la ciberseguridad del país mediante la creación de una estructura capaz de detectar, prevenir, responder y mitigar incidentes de seguridad cibernética. Este SOC se centrará en la monitorización continua de la infraestructura tecnológica de la entidad designada por la Corporación Colombia Digital, garantizando que se identifiquen y alerten sobre posibles amenazas en tiempo real. A través de una serie de protocolos definidos, el SOC estará preparado para gestionar la respuesta a incidentes de seguridad, lo que incluye la contención, erradicación y recuperación de sistemas afectados, minimizando así el impacto en la operación gubernamental.

La infraestructura del SOC se sustentará en aspectos estructurales basados en tecnologías de la información y comunicaciones centrados en los siguientes componentes:

- **Componente 1:** Gestión de Gobierno de Ciberseguridad
- **Componente 2:** Sistema y control de la superficie de ataque
- **Componente 3:** Plataformas de ciberinteligencia y huella digital
- **Componente 4:** Plataforma de ciberinvestigación global de amenazas

La integración de estos componentes con las plataformas tecnológicas existentes en la entidad designada por la Corporación Colombia Digital, así como el de diversas entidades gubernamentales permitirá un flujo de información efectivo y la coordinación necesaria para una respuesta rápida ante incidentes. Además, se establecerá un marco normativo que definirá las responsabilidades del SOC y las obligaciones de las diferentes entidades en materia de ciberseguridad, garantizando que todos los actores involucrados trabajen de manera coherente y alineada.

La capacitación del personal será un componente esencial en el desarrollo de la capacidad instalada del SOC. Se implementarán programas de formación continua para los analistas de seguridad y el personal encargado de operar el SOC, asegurando que estén actualizados en las últimas técnicas de respuesta a incidentes y en la gestión de vulnerabilidades. A su vez, se llevarán a cabo campañas de concienciación sobre ciberseguridad dirigidas a todos los empleados del gobierno, enfatizando la importancia de seguir buenas prácticas de seguridad para prevenir incidentes.

La colaboración interinstitucional será fundamental para el éxito del SOC Nacional. Se fomentará la cooperación entre diferentes entidades del gobierno, así como con fuerzas de seguridad y organismos internacionales, facilitando el intercambio de información sobre amenazas y mejores prácticas. La participación en redes de ciberseguridad, tanto a nivel nacional como internacional, permitirá al SOC acceder a inteligencia crítica que fortalecerá su capacidad de respuesta.

El SOC Nacional también deberá establecer mecanismos para la evaluación continua de sus operaciones. Esto incluirá auditorías regulares y la realización de simulacros de incidentes, lo que permitirá identificar áreas de mejora y garantizar que las estrategias implementadas sean efectivas ante la evolución constante de las amenazas cibernéticas. Además, se generarán informes regulares sobre la situación de la ciberseguridad en el país, proporcionando análisis de incidentes y tendencias, así como recomendaciones para la mejora de las prácticas de seguridad.

Finalmente, se establecerán líneas de comunicación directas entre la entidad designada por la Corporación Colombia Digital y las entidades gubernamentales, facilitando la notificación rápida de incidentes y la coordinación de respuestas. Este enfoque integral para la implementación de un SOC Nacional no solo mejorará la postura de ciberseguridad del gobierno de Colombia, sino que también contribuirá a generar confianza en los ciudadanos respecto a la seguridad de los servicios públicos y la protección de su información.

PORTAFOLIO DE SERVICIOS – COMPONENTES TÉCNICOS DEL SOC NACIONAL

El SOC Nacional de Colombia requiere una serie de servicios acompañados de tecnologías que permitan a la entidad designada por la Corporación Colombia Digital aumentar su capacidad de análisis y respuesta. Estos servicios deben ser capaces de detectar, analizar y mitigar amenazas en tiempo real, así como garantizar la continuidad del negocio y la protección de los datos críticos.

Estos nuevos servicios por incorporar en el portafolio de servicios de la entidad designada por la Corporación Colombia Digital incluyen los componentes de gestión de gobierno de ciberseguridad, el cual establece y mantiene políticas, procedimientos y controles para proteger la infraestructura tecnológica. Además, es crucial contar con el componente de sistemas y controles de la superficie de ataque que permitan identificar, analizar y mitigar vulnerabilidades y amenazas. Los servicios que abarcados por el componente de ciberinteligencia y huella digital son esenciales para monitorear y analizar la huella digital, así como para obtener información sobre posibles amenazas cibernéticas. Asimismo, un componente que abarque el servicio de ciberinvestigación global de amenazas la cual es necesaria para investigar y rastrear amenazas a nivel global, proporcionando información crítica para una defensa proactiva. La monitorización de información crítica garantiza la supervisión y protección de datos vitales para la organización. Así mismo, el componente de entrenamiento para equipos Red y Blue ofrece espacios y herramientas de simulación para preparar tanto a los equipos de defensa como a los de ataque, asegurando que el personal esté listo para enfrentar cualquier tipo de amenaza. Finalmente, el entrenamiento y transferencia de conocimiento de los componentes abarcados en este proyecto al equipo de trabajo de la entidad designada por la Corporación Colombia Digital, el cual es fundamental para la puesta en marcha y operaciones de estas nuevas capacidades. Todos estos componentes son fundamentales para el correcto funcionamiento y operación del SOC Nacional y para la protección integral de la infraestructura y los datos de la organización.

Figura 3: Estructura de los componentes para SOC Nacional
Fuente: Elaboración propia basado en las necesidades de la entidad designada por la Corporación Colombia Digital

A continuación, se relacionan los requerimientos que debe proporcionar la empresa proponente, para la implementación de cada uno de los componentes definidos en el alcance, cada componente debe contar con la estructura necesaria para su funcionamiento:

La composición de un componente de servicio tecnológico para el SOC Nacional implica una integración cuidadosa de hardware, software, procesos, datos y personal. Cada uno de estos elementos debe funcionar de manera sinérgica para garantizar la detección y respuesta efectiva ante amenazas cibernéticas, permitiendo al SOC cumplir con su misión de proteger los activos de información del gobierno. La implementación, mantenimiento y soporte técnico de estos componentes son esenciales para garantizar un servicio tecnológico de calidad en el ámbito de la ciberseguridad.

Figura 2: Elementos de un componente
Fuente: Elaboración propia basada en elementos teóricos de los fundamentos de Sistemas de Información

COMPONENTE PARA LA GESTIÓN DEL GOBIERNO DE CIBERSEGURIDAD

Este componente es esencial para establecer un marco robusto que proteja las infraestructuras críticas y los activos digitales del país, el cual debe integrar hardware, software, procesos, datos y personal para garantizar una gestión efectiva de la ciberseguridad. La empresa proponente será responsable de definir políticas cibernéticas específicas, desarrollar normas técnicas que aborden los riesgos sectoriales y establecer procedimientos de auditoría para evaluar la efectividad de las medidas implementadas. Además, se deben realizar análisis de posibles ataques para identificar sectores vulnerables, así como implementar métodos de evaluación continua que actualicen la clasificación de infraestructuras críticas. La capacitación del personal en protocolos de respuesta y la creación de un Plan de Recuperación de Desastres (DRP) integral serán fundamentales para asegurar una respuesta rápida y eficaz ante incidentes. Asimismo, la empresa proponente deberá facilitar foros de intercambio de información y mantener canales de comunicación permanentes, lo que permitirá una colaboración efectiva entre los distintos sectores críticos. Este enfoque integral no solo refuerza la seguridad cibernética, sino que también promueve una cultura de concienciación y resiliencia en el gobierno colombiano.

Para el cumplimiento de este componente la empresa proponente debe cumplir como mínimo los siguientes ítems en la solución aportada:

GESTIÓN DEL GOBIERNO	
ÍTEM	**DESCRIPCIÓN**
1.	Establecer los lineamientos para la creación de políticas cibernéticas específicas para infraestructuras críticas.
2.	Definir normas técnicas que aborden los riesgos de cada sector en el marco de las infraestructuras críticas.
3.	Desarrollar un proceso de auditoría que incluya revisiones técnicas y operativas sobre los operadores identificados.
4.	Realizar análisis de posibles ataques para identificar los sectores más vulnerables y sus principales operadores, con el fin de crear una red coordinada.
5.	Implementar métodos de evaluación continua para actualizar la clasificación de sectores críticos.
6.	Proporcionar guías técnicas detalladas para la implementación de medidas de seguridad, colaboración y coordinación.
7.	Establecer un plan medible y evaluable de incentivos para la implementación activa de estrategias de mitigación.
8.	Facilitar foros regulares para el intercambio de información y mejores prácticas entre sectores críticos.
9.	Crear la documentación para desarrollar campañas de concienciación que subrayen la importancia de la ciberseguridad en infraestructuras críticas.
10.	Adoptar una metodología estandarizada para evaluar pasivamente los riesgos de ciberseguridad en cada infraestructura crítica.
11.	Documentar la realización evaluaciones continuas de riesgos para ajustar la operación y capacidades ante las amenazas emergentes.
12.	Crear planes de tratamiento específicos para cada infraestructura crítica.
13.	Documentar los requerimientos para los sistemas de monitoreo continuo que sirvan para identificar nuevas amenazas y vulnerabilidades.
14.	Documentar la programación de revisiones periódicas de las estrategias de mitigación para asegurar su relevancia.

15.	Documentar la participación en programas de intercambio de inteligencia con agencias externas.
16.	Mantener una base de datos centralizada y segura que identifique y clasifique infraestructuras críticas.
17.	Facilitar el proceso de registro para nuevas infraestructuras críticas.
18.	Desarrollar protocolos claros de comunicación durante situaciones de emergencia.
19.	Desarrollar procedimientos para la respuesta a incidentes, detallando roles y actividades específicas.
20.	Desarrollar protocolos de comunicación claros tanto para el público como para las partes interesadas.
21.	Establecer los requerimientos y el proceso para contar con un equipo especializado en relaciones públicas para gestionar la percepción pública durante crisis.
22.	Asegurar el cumplimiento de normativas y regulaciones relacionadas con la ciberseguridad tanto a nivel nacional como internacional.
23.	Mantener canales de comunicación permanentes con entidades externas para coordinar respuestas efectivas.
24.	Proporcionar capacitación en el uso efectivo de los protocolos de coordinación.
25.	Alinear lo solicitado en este ítem al Modelo Integrado de Gestión de la entidad designada por la Corporación Colombia Digital, con base en los requerimientos técnicos solicitados para la adquisición de la membresía del Foro - FIRST (Forum of Incident Response and Security Teams)

PLAN DE RECUPERACIÓN DE DESASTRES (DRP)	
ÍTEM	**DESCRIPCIÓN**
1.	Entregar un Plan de Recuperación de Desastres (DRP) con procedimientos integrales para recuperar los servicios críticos y la tecnología de apoyo con rapidez y eficacia.
2.	Garantizar que el Plan de Recuperación de Desastres (DRP) permita establecer los procedimientos para recuperar los servicios de TI más críticos de la entidad designada por la Corporación Colombia Digital
3.	Asegurar que el Plan de Recuperación de Desastres (DRP) cuente con diferentes fases que demuestren y garanticen el proceso y su efectividad.
4.	Incluir, como mínimo, las siguientes fases en el Plan de Recuperación de Desastres (DRP): • **Fase Preventiva** • **Fase de Respuesta** • **Fase de Recuperación** • **Fase de Restauración**

IMPLEMENTACIÓN DEL COMPONENTE DE SISTEMA Y CONTROL DE LA SUPERFICIE DE ATAQUE

IMPLEMENTACIÓN DEL SISTEMA Y CONTROL DE LA SUPERFICIE DE ATAQUE	
ÍTEM	**DESCRIPCIÓN**
1.	El componente de nube provisto por la empresa proponente debe traducir la información obtenida mediante la evaluación de vulnerabilidades, evaluación de líneas base de configuración y evaluación de cumplimiento regulatorio sobre todos los activos TI, recursos en la nube, contenedores, aplicaciones web, sistemas de identidad y tecnología operativa (OT), con el fin de priorizar acciones y comunicar el riesgo cibernético.

2.	Teniendo en cuenta los servicios especializados del SOC Nacional y teniendo en cuenta que la entidad designada por la Corporación Colombia Digital cuenta con capacidades actuales que no soportan la operación y alcances de este proyecto, la empresa proponente deberá realizar migración/upgrade del software actual de Tenable One Standard a Tenable One Enterprise, esta debe cubrir un total mínimo de 16.200 activos, distribuidos de la siguiente manera: • Activos TI para VM: 5000 • Aplicaciones web: 200 • Identidades en el Directorio Activo: 5000 • Activos Cloud: 3000 • Activos OT: 3000 y 4 sensores
3.	El componente provisto por la empresa proponente debe soportar un módulo de flexibilidad que permita asignar recursos de acuerdo con las necesidades de evaluación y modificar dicha asignación siempre que sea necesario.
4.	El componente provisto por la empresa proponente deberá incluir capacitaciones del fabricante en dos tecnologías para 10 personas de la entidad.
5.	El componente provisto por la empresa proponente debe garantizar que el servicio de despliegue sea ejecutado directamente por el fabricante para mínimo 3 tecnologías quedando totalmente funcionales de acuerdo con el requerimiento de la entidad.
6.	El componente provisto por la empresa proponente debe proporcionar visibilidad completa sobre toda la superficie de ataque, a través de un único portal que proporcione una vista unificada.
7.	El componente provisto por la empresa proponente debe permitir anticipar las amenazas y priorizar los esfuerzos de mitigación para evitar ataques.
8.	El componente provisto por la empresa proponente debe permitir comunicar el riesgo cibernético para facilitar la toma de mejores decisiones.
9.	El componente provisto por la empresa proponente debe contar con una vista de exposición que permita enfocar los esfuerzos de seguridad, proporcionando información clara y concisa sobre la exposición en relación con la seguridad de la Entidad.
10.	El componente provisto por la empresa proponente debe proporcionar una puntuación global unificada de la exposición obtenida a partir de diferentes fuentes de datos.
11.	El componente provisto por la empresa proponente debe permitir análisis, visualización y priorización de rutas de ataques, proporcionando una respuesta enfocada de forma preventiva para interrumpir las rutas que pueden ser utilizadas por un atacante. Este análisis debe estar soportado por las criticidades expuestas en el marco MITRE ATT&CK.
12.	El componente provisto por la empresa proponente debe contar con un Inventario de Activos centralizado que proporcione visibilidad completa de todos los activos, independientemente de la fuente de datos (Activos TI, Activos Nube, Aplicaciones Web, Identidades del Directorio Activo), permitiendo la agrupación por medio de etiquetas.
13.	El componente provisto por la empresa proponente debe permitir gestionar la superficie de ataque externa, con el fin de identificar y reducir riesgos, brindando a la Entidad la visión de un atacante.
14.	El componente provisto por la empresa proponente debe realizar una gestión de vulnerabilidades basada en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas.
15.	El componente provisto por la empresa proponente debe realizar una evaluación de vulnerabilidades en entornos web de manera automatizada, completa y precisa.
16.	El componente provisto por la empresa proponente debe permitir la protección de la infraestructura en la nube, proporcionando visibilidad completa y continua de exposiciones, vulnerabilidades y permisos de acceso, priorizando tareas de remediación.
17.	El componente provisto por la empresa proponente debe permitir la protección del Directorio Activo, identificando brechas de seguridad, malas prácticas de configuración y ataques en tiempo real.

18.	El componente provisto por la empresa proponente debe permitir la evaluación comparativa de la exposición entre unidades de negocio o ubicaciones a nivel interno de la Entidad, así como con competidores de la industria a nivel externo, para obtener información que facilite la toma de decisiones certeras.
19.	El componente provisto por la empresa proponente debe soportar funcionalidades de seguridad con doble factor de autenticación.
20.	El componente provisto por la empresa proponente debe ser de un fabricante ubicado en el cuadrante de líderes de Gartner o Forrester en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).
21.	El componente debe contar con documentación, como datasheets, hojas de datos y/o manuales de usuario, que avalen el cumplimiento técnico de la solución ofertada.
22.	El componente provisto deberá contar con soporte del fabricante en un esquema 24 x 7 x 365.
23.	El componente provisto deberá proveerse como servicio en la nube o en formato de despliegue en premisa. (Máquinas virtuales o bare metal)
24.	El componente provisto no deberá requerir la instalación de agentes o software en los controladores de dominio ni la creación de cuentas con privilegios administrativos.
25.	El componente provisto deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
26.	El componente provisto por la empresa proponente debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
27.	El soporte de este componente provisto por la empresa proponente debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
28.	La empresa proponente provisto por la empresa proponente debe presentar certificación del fabricante que indique los productos y cantidades a utilizar en el componente.
29.	El componente provisto por la empresa proponente debe soportar funcionalidades de seguridad con doble factor de autenticación.
GESTIÓN DE VULNERABILIDADES	
ÍTEM	**DESCRIPCIÓN**
1.	El componente provisto por la empresa proponente para el servicio de nube provisto debe detectar, evaluar y priorizar las vulnerabilidades de los activos TI de la Entidad donde la entidad designada por la Corporación Colombia Digital ejecute a demanda la gestión de vulnerabilidades, formando parte de una plataforma de gestión de ciberexposición.
2.	El componente provisto por la empresa proponente debe tener la capacidad de cubrir más de 88.500 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.
3.	El componente provisto debe gestionar vulnerabilidades en sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores web, infraestructuras esenciales e infracciones de cumplimiento.
4.	El componente provisto por la empresa proponente debe proporcionar una consola de gestión en la nube para la gestión de la información de seguridad.
5.	El componente provisto por la empresa proponente debe ejecutar el descubrimiento de activos y vulnerabilidades mediante: • Monitoreo pasivo mediante análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Esta tecnología deberá estar patentada. • Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades, incluyendo el uso de IPv6. Estos sensores deben poder desplegarse como escáneres o agentes.

6.	El componente provisto por la empresa proponente debe utilizar sensores que puedan desplegarse en diversas plataformas, incluyendo Windows Workstations y Servers, Linux, Mac OS, ya sea en dispositivos virtuales o físicos.
7.	El componente provisto por la empresa proponente debe permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación, denotando la urgencia de atención a una vulnerabilidad. Esta calificación debe basarse en: • Correlación de información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación. • Predicción de la probabilidad de explotación futura de una vulnerabilidad. • Consideración de diversos elementos de evaluación, como la edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, y el tiempo transcurrido desde que se conoció una actividad de amenaza sobre la vulnerabilidad.
8.	El componente provisto por la empresa proponente debe permitir el despliegue del número de escáneres, monitores de red y agentes de escaneo necesarios sin incremento en costo.
9.	El componente provisto por la empresa proponente debe poder equilibrar cargas a través de múltiples escáneres de forma dinámica, basado en la disponibilidad de cada escáner desplegado.
10.	El componente provisto por la empresa proponente debe proporcionar una vista de soluciones que permita enfocar en las secciones más importantes primero, con los siguientes datos: • Descripción de la solución. • Número de dispositivos asociados a la solución. • Número de instancias de vulnerabilidades asociadas a la solución. • Calificación dinámica de probabilidad de explotación más alta para las vulnerabilidades asociadas a la solución.
11.	El componente provisto por la empresa proponente debe incluir la posibilidad de programar ventanas de escaneo.
12.	El componente provisto por la empresa proponente debe permitir etiquetar los activos por grupos en función de las necesidades de la organización, para categorizar los resultados y asignar las tareas correspondientes.
13.	El componente provisto por la empresa proponente debe contar con un esquema de perfiles de usuarios basados en roles, garantizando niveles adecuados de acceso a la plataforma.
14.	El componente provisto por la empresa proponente debe permitir la evaluación de vulnerabilidades y/o postura de seguridad de manera autenticada, utilizando credenciales como Windows, SSH y SNMPv3.
15.	El componente provisto por la empresa proponente debe contar con un módulo que permita la creación de filtros para mejorar las búsquedas, incluyendo por lo menos: protocolo, IP, activo, identificador de la vulnerabilidad, identificador CVE, CVSS, vulnerabilidades por su puntaje dinámico, explotabilidad, severidad.
16.	El componente provisto por la empresa proponente debe permitir la clasificación de activos identificados de manera manual o dinámica, basándose en diferentes atributos encontrados en el análisis, con etiquetas o grupos de trabajo, para su uso en escaneos posteriores.
17.	El componente provisto por la empresa proponente debe proporcionar información sobre la capacidad de explotación contra plataformas de validación como Metasploit, CoreImpact y Canvas.
18.	El componente provisto por la empresa proponente debe ejecutar escaneos de auditoría de cumplimiento mediante plantillas incluidas por defecto para sistemas como: Adtran AOS, Alcatel TiMOS, Amazon AWS, Arista EOS, entre otros.
19.	El componente provisto por la empresa proponente debe proporcionar plantillas de auditoría basadas en la política de cumplimiento de auditorías de CIS.
20.	El componente provisto por la empresa proponente debe tener la capacidad de integrarse con sistemas tipo SIEM para mejorar la visibilidad de amenazas y respuesta a vulnerabilidades. Por

	defecto, debe integrarse con soluciones como Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic.
21.	El componente provisto por la empresa proponente debe tener la capacidad de integrarse con soluciones tipo Privileged Access Management (PAM), pudiendo hacerlo de forma nativa al menos con los siguientes fabricantes: Arcon, Beyond Trust, Centrify, Cyber Ark, Hashi Corp, Thycotic.
22.	El componente provisto por la empresa proponente debe proporcionar integración con sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Debe soportar al menos Microsoft WSUS/SCCM, Red Hat Satellite, HCL BigFix, Symantec Altiris, Dell KACE K1000.

GESTIÓN DE VULNERABILIDADES EN APLICACIONES WEB	
ÍTEM	**DESCRIPCIÓN**
1.	El componente provisto por la empresa proponente para el servicio nube provisto por el contratista debe detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la Entidad, y debe ser provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades.
2.	El componente provisto por la empresa proponente debe ser capaz de escanear aplicaciones modernas desarrolladas en frameworks como JavaScript, AJAX, HTML5 y Single Page Applications.
3.	El componente provisto por la empresa proponente debe permitir observar las vulnerabilidades a lo largo del tiempo, clasificar estas según su nivel de riesgo, y alinearlas con el OWASP Top 10, además de proporcionar descripciones e instrucciones de remediación.
4.	El componente provisto por la empresa proponente debe ser de tipo SaaS, y también debe tener la capacidad de ser desplegada como un contenedor Docker, permitiendo el escaneo de sitios tanto públicos como privados.
5.	El componente provisto por la empresa proponente debe permitir realizar escaneos sin degradación del rendimiento del sitio, utilizando escaneos seguros, y debe permitir la exclusión de sitios a partir de la URL o extensiones de archivos.
6.	El componente provisto por la empresa proponente debe contar con escaneos predefinidos que permitan detectar rápidamente problemas de ciberhigiene, incluyendo: • SSL/TLS Scan • Config Audit Scan
7.	El componente provisto por la empresa proponente debe permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.
8.	El componente provisto por la empresa proponente debe soportar escaneos con autenticación avanzada, tales como: • HTTP Server Authentication • Web Application Authentication (Login Form, Cookie Authentication, Selenium Authentication, API Key, Bearer Authentication) • Client Certificate Authentication

9.	El componente provisto por la empresa proponente debe incluir las siguientes plantillas de escaneo: • API • Config Audit • log4Shell • Overview • PCI • Quick Scan • Scan • SSL/TLS
10.	El componente provisto por la empresa proponente debe permitir conocer el estado y progreso de una tarea de escaneo, además de generar tareas de escaneo programadas y enviar resultados por correo electrónico.
11.	El componente provisto por la empresa proponente debe contar con la capacidad de gestionar los hallazgos, permitiendo observar todas las vulnerabilidades descubiertas en la infraestructura.
12.	El componente provisto por la empresa proponente debe permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación, indicando la urgencia de atención a una vulnerabilidad.
13.	El componente provisto por la empresa proponente debe permitir una integración nativa con la solución de Gestión de Vulnerabilidades en Aplicaciones Web, posibilitando lanzar escaneos de vulnerabilidades y escaneos de sitios web de los activos descubiertos.
14.	El componente provisto debe identificar activos basados en: • Registros DNS • Direcciones IPs • ASN
15.	El componente provisto por la empresa proponente debe tener la capacidad de obtener información sobre la superficie de ataque externa en cuestión de minutos.
16.	El componente provisto por la empresa proponente debe categorizar activos con base en más de 200 campos de metadata, permitiendo la utilización de filtros.
17.	El componente provisto por la empresa proponente debe tener la capacidad de monitorear y notificar los cambios sobre los activos expuestos a internet de manera periódica, ya sea diaria o semanal.
18.	El componente provisto por la empresa proponente debe estar en la capacidad de descubrir dominios relacionados con los activos identificados y clasificados en el inventario de la solución, suministrando razones del porqué el dominio debería ser parte de la organización.
19.	El componente provisto por la empresa proponente debe permitir la administración de los activos de la organización, permitiendo el uso de filtros, etiquetas y tipos de datos.

20.	El componente provisto por la empresa proponente debe estar en la capacidad de notificar los cambios que se presenten sobre los activos del inventario mediante los siguientes medios: • Correo Electrónico • Slack • ServiceNow
21.	El componente provisto por la empresa proponente debe permitir incorporar un dominio sugerido al inventario.
22.	El componente provisto por la empresa proponente debe permitir el uso de subscripciones para notificar cambios sobre la superficie de ataque, incluyendo: • Identificación de nuevos servidores • Nuevos puertos abiertos o cerrados • Nuevo software
23.	El componente provisto por la empresa proponente debe contar con las siguientes subscripciones predefinidas: a. Compliance b. Exposición c. Geografía d. Higiene TI e. Marketing f. Tecnología
GESTIÓN DE INFRAESTRUCTURA EN LA NUBE	
ÍTEM	**DESCRIPCIÓN**
1.	El componente para el servicio nube provisto por la empresa proponente deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno de Identidades (CIEM), Análisis e Identificación de Comportamiento Malicioso (CDR) y Gobierno de Infraestructura como Código (IaC / DevSecOps) de la entidad, bajo una arquitectura CNAPP; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
2.	El componente provisto por la empresa proponente deberá soportar como mínimo con las nubes de Microsoft, Azure, Google y OCI.
3.	El componente provisto por la empresa proponente deberá poseer capacidades de autoremediación.
4.	El componente provisto por la empresa proponente deberá estar en la capacidad de evaluar y priorizar el riesgo de la infraestructura evaluada.
EVALUACIÓN DE EXPOSICIÓN DEL DIRECTORIO ACTIVO	
ÍTEM	**DESCRIPCIÓN**
1.	El componente para el servicio nube provisto por la empresa proponente debe auditar y monitorear de manera permanente la configuración del Directorio Activo de cualquier entidad de gobierno y/o privado para garantizar autonomía e imparcialidad en la detección de fallas, y debe ser provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades, formando parte de una plataforma de gestión de ciberexposición.

2.	El componente provisto por la empresa proponente debe ser de un fabricante tercero al del Directorio Activo que se va a monitorear, para garantizar una auditoría imparcial de un tercero con el objetivo de asegurar el Directorio Activo.
3.	El componente provisto por la empresa proponente debe proporcionar un análisis basado en grafos sobre las relaciones establecidas entre los diferentes objetos que componen el Directorio Activo, tales como usuarios, recursos y privilegios.
4.	El componente provisto por la empresa proponente no debe requerir la instalación de software o la activación de funcionalidades adicionales en el Directorio Activo a monitorear.
5.	El componente provisto por la empresa proponente debe ser capaz de inspeccionar y monitorear la configuración del Directorio Activo utilizando una cuenta de usuario con privilegios de lectura y visibilidad de los contenedores de objetos borrados y atributos de credenciales.
6.	El componente provisto por la empresa proponente debe mostrar gráficamente las relaciones dentro del Directorio Activo, permitiendo la evaluación de movimientos laterales desde activos potencialmente comprometidos.
7.	El componente provisto por la empresa proponente debe ser capaz de visibilizar, monitorear y analizar en tiempo real eventos que puedan afectar potencialmente al Directorio Activo.
8.	El componente provisto por la empresa proponente debe ser compatible con Azure Entra ID para expandir el alcance de las identidades en una organización, sin incurrir en costos adicionales.
9.	El componente provisto por la empresa proponente debe ser capaz de realizar auditorías en tiempo real sobre el Directorio Activo, alertando sobre posibles rutas de ataque y malas prácticas de configuración. Los hallazgos mínimos deben incluir: • Configuración débil del protocolo Netlogon • Certificados digitales asociados a cuentas privilegiadas • Controladores de dominio gestionados por usuarios ilegítimos • Uso de "primary group" • Configuración riesgosa de ADCS • Débiles políticas de credenciales • Delegación de Kerberos riesgosa • Falla de consistencia para "SDProp" • Cuentas privilegiadas ejecutando servicios de kerberos • Uso de algoritmos de cifrado débil en el servicio de PKI de Directorio Activo • Controladores de dominio falsos
10.	El componente provisto por la empresa proponente debe proporcionar información detallada sobre cada hallazgo, así como instrucciones detalladas sobre cómo corregir cada configuración no recomendada.
11.	El componente provisto por la empresa proponente debe soportar una cuenta señuelo cuyo único propósito es detectar a un atacante que intente comprometer la red a través de Active Directory.
12.	El componente provisto por la empresa proponente debe ser capaz de alertar automáticamente sobre el desarrollo de ataques dirigidos al Directorio Activo, tales como: • Ataques de enumeración • Golden ticket (Yara Detection, con capacidad de personalizar reglas Yara) • Password spraying • Dcsync • Dcshadow • OS Credential Dumping • PetitPotam • Explotación de DnsAdmins • Password guessing • Kerberoasting • Extracción de NTDS, entre otros.

13.	El componente provisto por la empresa proponente debe registrar en un repositorio independiente al Directorio Activo todos los cambios realizados a nivel de configuración.
14.	El componente provisto por la empresa proponente debe permitir la generación de alertas sobre comportamientos específicos en el Directorio Activo, definidos por el administrador de la plataforma.
15.	El componente provisto por la empresa proponente debe tener la capacidad de integrarse con sistemas tipo SIEM o SOAR para mejorar la visibilidad de amenazas y la respuesta a incidentes.
16.	El componente provisto por la empresa proponente debe generar alertas en formato syslog o por correo electrónico.

IMPLEMENTACIÓN DEL COMPONENTE DE PROTECCIÓN DE MARCA Y HUELLA DIGITAL

PROTECCIÓN DE MARCA Y HUELLA DIGITAL	
ÍTEM	**DESCRIPCIÓN**
1.	El componente para el servicio nube provisto por la empresa proponente debe cubrir hasta 500 dominios para la funcionalidad de Credenciales.
2.	El componente nube provisto por la empresa proponente debe cubrir hasta 5120 IPs para la funcionalidad de Credenciales.
3.	El componente nube provisto por la empresa proponente debe cubrir hasta 500 dominios para la funcionalidad de Dark Web y Hacktivismo.
4.	El componente nube provisto por la empresa proponente debe cubrir hasta 5120 IPs para la funcionalidad de Dark Web y Hacktivismo.
5.	El componente nube provisto por la empresa proponente debe cubrir hasta 150 keywords para la funcionalidad de Dark Web y Hacktivismo.
6.	El componente nube provisto por la empresa proponente debe cubrir hasta 500 dominios para la funcionalidad de Protección de Dominios.
7.	El componente nube provisto por la empresa proponente debe cubrir hasta 150 keywords para la funcionalidad de Protección de Dominios.
8.	El componente nube provisto por la empresa proponente debe cubrir hasta 150 keywords para la funcionalidad de Medios Sociales, Filtraciones de Datos, y Aplicaciones Móviles.
9.	El componente nube provisto por la empresa proponente debe proporcionar almacenamiento en la nube de hasta 300 GB.
10.	El componente provisto por la empresa proponente debe tener la capacidad de recopilar datos de amenazas desde múltiples fuentes, incluyendo fuentes abiertas, cerradas y privadas.
11.	El componente provisto por la empresa proponente debe poder analizar los datos recopilados de manera automática.
12.	El componente provisto por la empresa proponente debe correlacionar los datos de amenazas para identificar patrones y tendencias.
13.	El componente provisto por la empresa proponente debe proporcionar datos enriquecidos sobre amenazas en tiempo real.
14.	El componente provisto por la empresa proponente debe cubrir una variedad de categorías de amenazas, adaptándose a diferentes tipos de ciberataques.
15.	El componente provisto por la empresa proponente debe automatizar la recolección de datos de amenazas desde fuentes abiertas.
16.	El componente provisto por la empresa proponente debe automatizar la recolección de datos de amenazas desde fuentes cerradas.
17.	El componente provisto por la empresa proponente debe automatizar la recolección de datos de amenazas desde fuentes privadas.

18.	El componente provisto por la empresa proponente debe procesar los datos de amenazas de manera eficiente y rápida.
19.	El componente provisto por la empresa proponente debe enriquecer los datos recopilados para ofrecer una visión completa y detallada de las amenazas.
20.	El componente provisto por la empresa proponente debe contar con una plataforma de inteligencia sobre ciberamenazas que sea accionable y específica.
21.	El componente provisto por la empresa proponente debe ser fácilmente instalable, sin necesidad de agentes, y completamente SaaS.
22.	El componente provisto por la empresa proponente debe contar con un historial de al menos 13 años de datos sobre ciberamenazas.
23.	El componente provisto por la empresa proponente debe permitir la ampliación de características de forma ágil y rápida.
24.	El componente provisto por la empresa proponente debe permitir la reducción de características según las necesidades del usuario.
25.	El componente provisto por la empresa proponente debe ser escalable para adaptarse a las circunstancias cambiantes del sector.
26.	El componente provisto por la empresa proponente debe ser modular, permitiendo la integración de nuevas capacidades y ventajas según sea necesario.
27.	El componente provisto por la empresa proponente debe ser compatible con plugins para SIEM.
28.	El componente provisto por la empresa proponente debe ser compatible con plugins para SOAR.
29.	El componente provisto por la empresa proponente debe ser compatible con plugins para TIP.
30.	El componente provisto por la empresa proponente debe permitir la integración de datos de amenazas STIX/TAXII.
31.	El componente provisto por la empresa proponente debe permitir el intercambio de información de amenazas de manera segura y eficiente.
32.	El componente provisto por la empresa proponente debe detectar credenciales filtradas en mercados clandestinos.
33.	El componente provisto por la empresa proponente debe detectar credenciales robadas obtenidas por malware.
34.	El componente provisto por la empresa proponente debe enfocarse en la detección de credenciales tipo Botnet.
35.	El componente provisto por la empresa proponente debe proporcionar visibilidad en tiempo real de las credenciales filtradas o robadas.
36.	El componente provisto por la empresa proponente debe proporcionar visibilidad sobre las actividades maliciosas dirigidas a la organización en la web oscura.
37.	El componente provisto por la empresa proponente debe generar inteligencia sobre ciberdelincuentes mediante el uso de palabras clave específicas.
38.	El componente provisto por la empresa proponente debe incluir, como mínimo, las siguientes fuentes/foros: Exploit.IN, xss.is, russianmarket.to, leakzone.net, LeakBase, Demonforums.net, Sinisterly, BHF.ee, zelenka.guru, Hack Forums, Nulled, Altenen - Trust and Safety, cracking.org, Cracking Pro, rstforums.com, Cracked.io - Beyond the Limits, Hack Forums, Cracking Pro, Crackia, Игровой портал – YouHack.
39.	El componente provisto por la empresa proponente debe descubrir documentos confidenciales de la organización que hayan sido expuestos en internet.
40.	El componente provisto por la empresa proponente debe monitorizar el código fuente de la organización que haya sido filtrado en la web profunda o redes P2P.
41.	El componente provisto por la empresa proponente debe medir la intencionalidad de la filtración de documentos internos compartidos con proveedores de intercambio de archivos.

42.	El componente provisto por la empresa proponente debe incluir, como mínimo, las siguientes fuentes: GitHub, GitLabs, Postman, Gitlabs, Bitbucket, Google Docs, S3Buckets.
43.	El componente provisto por la empresa proponente debe monitorizar la actividad global relacionada con el hacktivismo en redes sociales.
44.	El componente provisto por la empresa proponente debe anticiparse a los ataques mediante el descubrimiento de dominios potencialmente fraudulentos utilizando técnicas de typosquatting.
45.	El componente provisto por la empresa proponente debe supervisar la ciberocupación que pueda afectar a la infraestructura de la organización.
46.	El componente provisto por la empresa proponente debe incluir un sistema de alerta temprana para detectar amenazas emergentes.
47.	El componente provisto por la empresa proponente debe contar con un geolocalizador activo para proteger contra vectores de ataque específicos.
48.	El componente provisto por la empresa proponente debe incluir, como mínimo, las siguientes fuentes: LeakIX, Shodan.
49.	El componente provisto por la empresa proponente debe detectar aplicaciones no autorizadas que utilicen activos de la empresa.
50.	El componente provisto por la empresa proponente debe monitorizar la huella digital de la organización en redes sociales y motores de búsqueda.
51.	El componente provisto por la empresa proponente debe detectar páginas no autorizadas que utilicen marcas, logotipos o activos de la organización.
52.	El componente provisto por la empresa proponente debe incluir, como mínimo, las siguientes fuentes: Mastodon, YouTube, Twitter (X), Facebook, WeChat.
HUELLA DIGITAL	
ÍTEM	**DESCRIPCIÓN**
1.	El componente nube provisto por la empresa proponente debe identificar fallas y vulnerabilidades en los dominios de seguridad clave que incluyan seguridad de red, seguridad de aplicaciones, integridad de DNS, seguridad de punto final, reputación de IP, cadencia de parches, canales de piratería, y fugas de información y phishing.
2.	El componente nube provisto por la empresa proponente debe detectar los hallazgos a través de fuentes de datos activas, pasivas y de terceros, incluyendo métodos activos de recopilación de datos con sensores que exploren Internet en busca de vulnerabilidades y debilidades de seguridad.
3.	El componente nube provisto por la empresa proponente debe incluir métodos pasivos como sumideros, honeypots, y recopilación de datos de intercambios publicitarios, complementados por fuentes de terceros, para proporcionar una imagen completa de los controles de seguridad de las empresas que se supervisan.
4.	El componente nube provisto por la empresa proponente debe tener la capacidad de monitorear la huella digital de hasta 50 dominios los cuales se podrá poder distribuir en diferentes entidades a nivel nacional.
5.	El componente provisto por la empresa proponente debe incluir a los principales proveedores seleccionados y ser capaz de catalogar rápidamente nuevos proveedores, describiendo la cobertura actual del servicio en términos de empresas, dominios e IPs, y el tiempo necesario para evaluar una nueva empresa.
6.	El componente provisto por la empresa proponente debe respaldar la evidencia de los hallazgos en la plataforma y los terceros utilizados, utilizando fuentes como WHOIS, certificados SSL, búsqueda de DNS, datos publicados y fuentes de datos de terceros para el proceso de evaluación.

7.	El componente provisto por la empresa proponente debe proporcionar una forma de visualizar posibles infracciones existentes, sistemas comprometidos y datos que indiquen la transferencia de archivos entre pares.
8.	El componente provisto por la empresa proponente debe compartir información detallada con cualquier tercero que esté siendo monitoreado, incluyendo la dirección IP, fuente de datos, descripción de la vulnerabilidad, riesgo, recomendación de parche, enlaces a fuentes de información de parche, fechas de detección, última observación e impacto en la puntuación.
9.	El componente provisto por la empresa proponente debe permitir la identificación de posibles vulnerabilidades que puedan ser observadas externamente, así como el tiempo durante el cual están activas.
10.	El componente provisto por la empresa proponente debe ofrecer la posibilidad de ajustar los activos digitales identificados por las empresas, incluso después de una fusión o adquisición, para obtener resultados actualizados y precisos.
11.	El componente provisto por la empresa proponente debe proporcionar capacidades analíticas profundas, incluyendo la capacidad de comprender el desempeño relativo de la organización en comparación con sus pares.
12.	El componente provisto por la empresa proponente debe proporcionar una visión forense profunda para analizar posibles problemas tanto en la infraestructura propia como en el seguimiento de terceros.
13.	El componente provisto por la empresa proponente debe incluir una herramienta para predecir modificaciones y realizar simulaciones de cambios de calificación.
14.	El componente provisto por la empresa proponente debe incluir la Calificación de Riesgo Cibernético con actualizaciones diarias para cada entidad monitoreada.
15.	El componente provisto por la empresa proponente debe realizar escaneos automáticos de vulnerabilidades con una duración máxima de 31 días.
16.	El componente provisto por la empresa proponente debe evaluar individualmente cada vector de riesgo que compone la clasificación.
17.	El componente provisto por la empresa proponente debe garantizar que la correlación entre violaciones de datos y la calificación de riesgo cibernético haya sido validada independientemente por un tercero.
18.	El componente provisto por la empresa proponente debe respaldar todos los eventos que impacten en la calificación con evidencia objetiva y verificable, que además permita actuar sobre ellos.
19.	El componente provisto por la empresa proponente debe permitir la visualización completa de la huella digital de todos los vendedores monitoreados, con evidencias detalladas.
20.	El componente provisto por la empresa proponente debe escanear todas las IPs, propias o de terceros, como máximo cada 45 días, con fecha de validación en la solución.
21.	El componente provisto por la empresa proponente debe incluir una solución nativa para enviar y recibir cuestionarios de seguridad personalizados en español, completamente personalizable.
22.	El componente provisto por la empresa proponente debe permitir la creación de puntuaciones personalizadas por huella digital y/o localización de IPs.
23.	El componente provisto por la empresa proponente debe incluir una herramienta nativa del plan de acción para reflejar la mejora de la puntuación.
24.	El componente provisto por la empresa proponente debe remediar vulnerabilidades o eventos detectados que impacten la puntuación en no más de 48 horas.
25.	El componente provisto por la empresa proponente debe permitir establecer acciones automáticas ante nuevas vulnerabilidades, eventos o incidentes.
26.	El componente provisto por la empresa proponente debe hacer pública la metodología, cálculo y algoritmo utilizados, disponibles en internet.

27.	El componente provisto por la empresa proponente debe contar con un sistema de marcado (tags) para cada entidad monitoreada.
28.	El componente provisto por la empresa proponente debe permitir la visualización general de las entidades monitoreadas con su puntaje y variación en los últimos 30 días.
29.	El componente provisto por la empresa proponente debe recopilar datos de los registros SPF, TLS/SSL, vulnerabilidades SSL/TLS, encabezados de aplicaciones web, redirección HTTP/HTTPS, servicios en puertos abiertos, registros DNSSEC, software de servidores, vulnerabilidades en servicios expuestos, y exposición de servidores Bitcoin.
30.	El componente provisto por la empresa proponente debe clasificar los datos recopilados basándose en estándares como CISv8, CSA-CCM, ISO/IEC 27001:2022, NIST CSF, SOC2.
31.	El componente provisto por la empresa proponente debe identificar servicios en puertos abiertos, aunque el número de puerto no sea estándar.
32.	El componente provisto por la empresa proponente debe identificar terceros o cuartos en una organización.
33.	El componente provisto por la empresa proponente debe proporcionar acceso ilimitado a la plataforma para un proveedor.
34.	El componente provisto por la empresa proponente debe mostrar rápidamente qué proveedores tienen infecciones.
35.	El componente provisto por la empresa proponente debe mostrar rápidamente qué proveedores tienen vulnerabilidades.
36.	El componente provisto por la empresa proponente debe permitir el acceso a la plataforma para proveedores por invitación, con apoyo del fabricante durante el acceso y la posibilidad de impugnar descubrimientos.
37.	El componente provisto por la empresa proponente debe demostrar de manera transparente el porcentaje de impacto que una vulnerabilidad tiene en el puntaje tanto de la entidad designada por la Corporación Colombia Digital como de cualquier tercero monitoreado.
38.	El componente provisto por la empresa proponente debe incluir una corrección de pronóstico (remediación) para indicar mejoras en la calificación si se toman acciones específicas.
39.	El componente provisto por la empresa proponente debe actualizar automáticamente la huella digital de todas las empresas mapeadas en el portal/solución al menos cada 45 días.
40.	El componente provisto por la empresa proponente debe contar con al menos 12,000,000 de empresas/entidades/organizaciones mapeadas en el portal y disponibles para monitoreo inmediato.
41.	El componente provisto por la empresa proponente debe mapear una nueva empresa/organización/entidad en un tiempo máximo de 10 minutos para que esté disponible en el portal.
42.	El componente provisto por la empresa proponente debe permitir a la entidad designada por la Corporación Colombia Digital visualizar toda la huella digital de cualquier tercero monitoreado, sin necesidad de autorización.
43.	El componente provisto por la empresa proponente debe proporcionar datos forenses detallados de eventos detectados para cualquier tercero monitoreado.
44.	El componente provisto por la empresa proponente debe visualizar el porcentaje de impacto de cada vulnerabilidad en la puntuación o calificación.
45.	El componente provisto por la empresa proponente debe asegurar que las direcciones IP no sean excluidas sin la documentación suficiente, para evitar la manipulación de la calificación.
46.	El componente provisto por la empresa proponente debe basar la comparación de vulnerabilidades en empresas con un número similar de IPs.
47.	El componente provisto por la empresa proponente debe ofrecer un proceso completamente interactivo para ajustar las colecciones digitales en la plataforma, con capacidad para eliminar y agregar direcciones IP, y generar cuadros de mando personalizados.

48.	El componente provisto por la empresa proponente referente a la tecnología utilizada debe ser considerada líder por al menos un analista o firma independiente como Forrester o Gartner.

IMPLEMENTACIÓN DEL COMPONENTE DE CIBERINVESTIGACIÓN GLOBAL DE AMENAZAS

CIBERINVESTIGACIÓN Y ANÁLISIS DE AMENAZAS	
ÍTEM	**DESCRIPCIÓN**
1.	El componente nube provisto por la empresa proponente debe contar con una plataforma de ciberinvestigación de amenazas diseñada para neutralizar amenazas de manera eficiente y efectiva.
2.	El componente nube provisto por la empresa proponente debe facilitar la aceleración de las operaciones de seguridad.
3.	El componente nube provisto por la empresa proponente debe permitir consolidar en una única vista todas las amenazas internas y externas.
4.	El componente provisto por la empresa proponente debe priorizar las amenazas, automatizar su manejo y colaborar con terceros.
5.	El componente provisto por la empresa proponente debe ser capaz de recopilar, analizar y, cuando sea necesario, extraer información sobre las amenazas detectadas.
6.	El componente provisto por la empresa proponente debe unificar los datos provenientes de múltiples fuentes, incluyendo feeds OSINT, feeds comerciales de terceros, feeds de correlacionadores, feeds de vulnerabilidades y feeds de vigilancia cibernética.
7.	El componente provisto por la empresa proponente debe incluir un módulo de biblioteca de amenazas capaz de puntuar y priorizar automáticamente la inteligencia con base en ciertos parámetros.
8.	El componente provisto por la empresa proponente debe proporcionar al menos un contexto de perspectiva de la amenaza.
9.	El componente provisto por la empresa proponente debe permitir la priorización automática basada en todas las fuentes y el enriquecimiento de estas.
10.	El componente provisto por la empresa proponente debe incluir un banco de trabajo que permita integrar las capacidades humanas con la automatización en inteligencia de amenazas.
11.	El componente provisto por la empresa proponente debe proporcionar una detección rápida y proactiva.
12.	El componente provisto por la empresa proponente debe permitir una integración efectiva de los procesos con la plataforma.
13.	El componente provisto por la empresa proponente debe disponer de un market place de integraciones con componentes propios como SDK/API.
14.	El componente provisto por la empresa proponente debe ofrecer soporte para STIX/TAXII.
15.	El componente provisto por la empresa proponente debe incluir un módulo de investigación que permita la fusión de datos como amenazas, evidencias y objetos para realizar un análisis y comprensión proactiva de la postura de seguridad.
16.	El componente provisto por la empresa proponente debe ofrecer herramientas de visualización y documentación en un entorno compartido dentro del módulo de investigación.
17.	El componente provisto por la empresa proponente debe incluir una plataforma de compartición de ciberinteligencia que permita compartir de manera segura indicadores de interés con otros grupos como CERT, SOC o CSIRT.
18.	El componente provisto por la empresa proponente debe poder interactuar de manera bidireccional con MXDR para facilitar o activar flujos de trabajo con la infraestructura de seguridad.

19.	El componente provisto por la empresa proponente debe contar con una REST-API potente y un SDK basado en Python.
20.	El componente provisto por la empresa proponente debe incluir un marco de ingesta de feeds y capacidades de exportación.
21.	El componente provisto por la empresa proponente debe permitir crear y almacenar tipos de datos personalizados como información relacionada con fraudes y tarjetas de crédito robadas.
22.	El componente provisto por la empresa proponente debe permitir realizar búsquedas profundas y detalladas en los datos para identificar patrones y tendencias.
23.	El componente provisto por la empresa proponente debe ofrecer la capacidad de generar cuadros de mando completamente personalizables para analizar datos y hacer seguimiento de amenazas.
24.	El componente provisto por la empresa proponente debe enriquecer la inteligencia de fuentes internas y externas.
25.	El componente provisto por la empresa proponente debe permitir consultar herramientas y realizar cambios operativos desde un único sistema.
26.	El componente provisto por la empresa proponente debe permitir ajustar los niveles de confianza y gravedad de las fuentes.
27.	El componente provisto por la empresa proponente debe permitir comparar fuentes de amenazas para evaluar su valor.
28.	El componente provisto por la empresa proponente debe permitir colaborar en investigaciones con otros miembros del equipo.
29.	El componente provisto por la empresa proponente debe contar con un modelo de datos flexible basado en STIX 2.0.
30.	El componente provisto por la empresa proponente debe permitir recopilar, ingerir y procesar información relevante según los casos de uso específicos.
31.	El componente provisto por la empresa proponente debe permitir el acceso mediante una interfaz web.
32.	El componente provisto por la empresa proponente debe ofrecer integraciones bidireccionales con otras fuentes.
33.	El componente provisto por la empresa proponente debe ser compatible con integraciones con sistemas SIEM, SOAR, Sandbox, Ticketing, Big Data, MISP, Service Desk, IPS, Firewall, EDR y Vulnerabilidades.
34.	El componente provisto por la empresa proponente debe permitir el uso de datos almacenados en bibliotecas de amenazas.
35.	El componente provisto por la empresa proponente debe tener un motor de ciberinvestigación de amenazas capaz de ingerir y agregar datos estructurados y no estructurados a través de aplicaciones de Marketplace y una API abierta.
36.	El componente provisto por la empresa proponente debe normalizar automáticamente datos de diferentes fuentes, formatos e idiomas en un único objeto.
37.	El componente provisto por la empresa proponente debe correlacionar datos atómicos para identificar relaciones y ofrecer una visión unificada.
38.	El componente provisto por la empresa proponente debe permitir la priorización mediante una puntuación dinámica controlada por el cliente para asegurar la relevancia y filtrar el ruido.
39.	El componente provisto por la empresa proponente debe permitir traducir los datos al formato y al idioma necesarios para su uso en todos los sistemas.
40.	El componente provisto por la empresa proponente debe permitir visualizar la cronología de incidentes, adversarios y campañas.
41.	El componente provisto por la empresa proponente debe contar con capacidades avanzadas para la creación de cuadros de mando personalizables, con posibilidad de desglosar información en tiempo real.

42.	La empresa proponente debe presentar una certificación emitida directamente por el fabricante utilizado para la prestación del servicio que acredite que es un distribuidor autorizado en Colombia y que cuenta con la capacidad de brindar soporte con al menos dos años de experiencia.
MANTENIMIENTO DE PLATAFORMA MISP - MALWARE INFORMATION SHARING PLATFORM	
ÍTEM	**DESCRIPCIÓN**
1.	La empresa proponente debe brindar el mantenimiento de la plataforma MISP (Malware Information Sharing Platform) con la que actualmente cuenta la entidad designada por la Corporación Colombia Digital, permitiendo la compartición de información de inteligencia de amenazas a nivel global con otros grupos de interés, incluyendo organizaciones la entidad designadas por la Corporación Colombia Digital y otras organizaciones nacionales, regionales o globales.
2.	El componente debe permitir la valoración automática del tiempo de vida de los indicadores y la gestión automática de estos.
3.	El componente debe tener la capacidad de recibir información mediante su conector nativo con una plataforma de inteligencia de amenazas (TIP).
4.	El componente debe permitir la publicación de dichas amenazas con los grupos de interés seleccionados.
5.	El componente debe consolidar las amenazas compartidas desde estos grupos en una plataforma TIP.
6.	El componente debe ser capaz de almacenar información tanto técnica como no técnica sobre malware y ataques ya detectados.
7.	El componente debe poder crear automáticamente relaciones entre eventos y sus atributos, identificando amenazas relacionadas.
8.	El componente debe permitir generar reglas para la detección o prevención de amenazas a partir de indicadores para sistemas NIDS (Network Intrusion Detection System).
9.	El componente debe almacenar datos en un formato estructurado, permitiendo un uso automatizado de la base de datos para alimentar sistemas de detección o herramientas forenses.
10.	El componente debe permitir compartir los atributos de eventos maliciosos, malware y amenazas con otras organizaciones y grupos de confianza.
11.	El componente debe incluir capacidades para el modelado y estructuración de eventos y amenazas según estándares de intercambio de incidentes, como STIX.
12.	El componente debe permitir establecer una arquitectura federada entre comunidades para intercambiar información entre comunidades de forma segura y controlada.
13.	El componente debe permitir integrarse con nuevos CSIRT sectoriales, privados y homólogos internacionales, ampliando así la red de intercambio de información sobre amenazas.
14.	El componente provisto por la empresa proponente debe ser compatible y tener la capacidad de conectarse con la mayoría de las plataformas de inteligencia de amenazas y soluciones de seguridad.

INTEGRACIÓN DE HERRAMIENTAS

La empresa proponente debe garantizar la interoperabilidad entre las siguientes plataformas y herramientas que hoy existen en la entidad designada por la Corporación Colombia Digital. La integración debe facilitar el intercambio eficiente de datos y eventos de seguridad entre estas herramientas, utilizando interfaces de programación de aplicaciones (APIs) y protocolos de comunicación estándares y/o nativos.

- Herramienta para el análisis de vulnerabilidades en infraestructura cloud e Infraestructura on-premises. Tenable One Standard.
- Herramienta para Ciberinteligencia de Amenazas - Mandiant Threat Intelligence Fusión.
- Herramienta para Análisis de Malware Sandbox Trellix DoD – Sitio WEB de la entidad designada por la Corporación Colombia Digital
- Herramienta Helix Enterprise Edition
- Plataforma Malware Information Sharing Platform (MISP)
- Plataforma de Gestión de Incidentes RTIR.

Las herramientas anteriormente descritas deben interconectarse con el componente de ciberinvestigación global de amenazas provistas por la empresa proponente, mínimo en los siguientes componentes.

- Ciberinvestigación Global de Amenazas
- Monitorización de Información Crítica
- Entrenamiento para Equipos Red Y Blue
- Protección de Marca y Huella Digital
- Sistema Y Control De La Superficie De Ataque

UBICACIÓN DEL SOC NACIONAL

El SOC Nacional se deberá instalar en todos sus componentes y adecuaciones en las instalaciones del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, ubicado en la ciudad de Bogotá D.C., Cra 8 entre calles 12a y 12b, Edificio Murillo Toro.

SOPORTE TÉCNICO Y DERECHOS DE USO DE LOS ELEMENTOS DE HARDWARE Y DE SOFTWARE DE LOS COMPONENTES DESCRITOS EN EL PROYECTO

Los elementos software y hardware de cada uno de los compontes provistos por la empresa proponente debe asegurar que cuenten con los permisos de uso del fabricante garantizando los derechos de autor de los elementos, así como el soporte técnico de los mismos por un periodo de doce (12) meses, estos derechos de uso deben incluir actualizaciones a las versiones más recientes durante el período solicitado.

Así mismo debe realizar la configuración y afinamiento inicial junto con el personal de la entidad designada por la Corporación Colombia Digital, garantizando la correcta implementación de sus funcionalidades y el entendimiento de la operación y alcances definidos en la normatividad vigente.

El soporte técnico debe ser realizado directamente por el fabricante, a cada una de las soluciones, herramientas y plataformas provistas en cada componente, el cual debe prestarse en la modalidad 7x24x365, para lo cual deberá entregar los respectivos protocolos de escalamiento de problemas.

EQUIPO DE TRABAJO

Durante la vigencia del contrato la empresa proponente pondrá a disposición de la entidad designada por la Corporación Colombia Digital un equipo consultor que brindará apoyo frente a la documentación que pueda generarse a partir del análisis y evaluación de las infraestructuras críticas desde la entidad designada por la Corporación Colombia Digital.

Así mismo, la empresa proponente debe garantizar un equipo de trabajo para los componentes solicitados en el presente anexo técnico.

El equipo mínimo requerido deberá ser el siguiente:

PERFIL	CANTIDAD	FORMACION ACADEMICA Y PROFESIONAL	EXPERIENCIA ESPECIFICA	DEDICACION A LA FASE DE IMPLEMENTACION
Gerente de Proyectos	1	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. • Especialista en Gerencia de proyectos • PMP • Scrum Master	Experiencia como Gerente de proyectos de seguridad de la información o seguridad informática de por lo menos dos (2) años.	100%
Consultor de seguridad uno	1	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. Con posgrado en seguridad de la información o seguridad informática o ciberseguridad o ciberdefensa o afines. Debe contar mínimo con las siguientes certificaciones • Lead CyberSecurity Professional Certification - LCSPC • Auditor Líder ISO 27001:2022 • Certified Ehtical Hacker-EC-Council	Experiencia como director de operaciones de seguridad de la información o seguridad informática de tres (3) años.	100%

		• Cyber Security Foundation Professional Certificate – CSFPC • Scrum Master • ISO 22301:2019 Auditor interno		
Especialista en Inteligencia de amenazas	1	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. Debe contar mínimo con las siguientes 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	100%

PERFIL	CANTIDAD	FORMACION ACADEMICA Y PROFESIONAL	EXPERIENCIA ESPECIFICA	
Consultor de seguridad	1	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. Con posgrado en auditoria de sistemas o seguridad de la información o seguridad informática o ciberseguridad o ciberdefensa Debe contar mínimo con las siguientes Certificaciones: • Lead Risk Manager ISO 31000 • 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	Experiencia en seguridad informática de tres (3) años y por lo menos un año de experiencia en labores relacionas con SOC	100%

Consultor de seguridad	1	Profesional en Ingeniería de Sistemas, Ingeniero de computación, Ingeniero electrónico, Ingeniero de telecomunicaciones, Ingeniero en informática. Con posgrado en seguridad de la información o seguridad informática o ciberseguridad o ciberdefensa Debe contar mínimo con las siguientes Certificaciones • Auditor Líder ISO 27001:2013 • Implementador Líder ISO 27001:2013 • Certified Information Systems Auditor CISA • Certified Information Security Manager CISM • Risk Manager ISO 31000:2018 • CBCP	Experiencia en seguridad de la información o seguridad informática de tres (3) años y por lo menos un año de experiencia en labores relacionas con la oficina de seguridad de la información.	100%

Nota: Cuando por cualquier circunstancia, fuerza mayor o caso fortuito se requiera cambiar un integrante del equipo de trabajo requerido, el nuevo integrante debe contar el perfil establecido o superior y la hoja de vida debe ser remitida al supervisor del contrato a efecto de aprobar la misma, con un mínimo de cinco (5) días calendario.

ACUERDOS DE NIVELES DE SERVICIO – ANS

La disponibilidad se medirá usando la siguiente ecuación:

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

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 de la entidad designada por la Corporación Colombia Digital en cualquier momento durante la ejecución del contrato. La información mantenida por el proveedor le debe permitir a la entidad designada por la Corporación Colombia Digital, 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

ANS	
Disponibilidad exigida herramientas >=99.99% mensual	
Interrupciones	

Hace referencia al 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 de la entidad designada por la Corporación Colombia Digital en cualquier momento durante la ejecución del contrato. La información mantenida por el proveedor le debe permitir Al Equipo de la entidad designada por la Corporación Colombia Digital verificar el número de Interrupciones histórico de meses anteriores y el número de Interrupciones acumuladas para el mes en curso.
La medición se hace de forma individual sobre cada herramienta. Es decir, cada herramienta debe cumplir con el valor exigido en el ANS.

ANS	
Interrupciones máximas en un mes:	2 interrupciones
Efectividad en resolución de incidentes/solicitudes:	

Mide el nivel de cumplimiento del total de solicitudes recibidas en un periodo de un mes 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 de la entidad designada por la Corporación Colombia Digital 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 definido
---------- X 100
Total de Solicitudes recibidas (Llamadas, chat, registros o email)

ANS	Tiempo

Efectividad en la atención >= 90%	Prioridad 1: Efectividad de resolución <=2 horas Prioridad 2: Efectividad de resolución <= 4 horas Prioridad 3: Efectividad de resolución <= 8 horas

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, alineado con lo definido en lo referente a Seguridad y Privacidad de la Información por parte del Ministerio TIC, 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 de la entidad designada por la Corporación Colombia Digital a la cual tengan acceso.

Cumplimiento de la Política de Seguridad de la entidad designada por la Corporación Colombia Digital

El proveedor se debe alinear y cumplir lo establecido en el Sistema de Gestión de la Seguridad de la información que viene implementando el Ministerio TIC, y dar cumplimiento a la Resolución 0448 de 2022, la cual actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, 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."

De igual manera, a los parámetros establecidos por la Subdirección Administrativa en la Política de Gestión de Activos (Inventario de activos, Protección, Archivos de Gestión, Clasificación de la Información, y firma de documentos) descritos en el Artículo 6 de la resolución señalada.

https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de- Privacidad-y-Condiciones-de-Uso

Políticas de Borrado Seguro

El proponente seleccionado deberá realizar el borrado seguro de cada uno de los dispositivos que sean utilizados en cualquiera de los servicios a desplegarse en las entidades, como parte de la ejecución del contrato.

Al finalizar la ejecución contractual el proponente seleccionado, deberá allegar con firma del representante legal, una certificación en la cual se evidencie que en todos los casos en donde se tuvo registro de información y datos de las entidades, fueron objeto de las políticas de borrado seguro, de tal forma que garantice que la información gestionada, almacenada fue eliminada en su totalidad y que no queda ninguna copia o elemento que permita realizar un proceso de recuperación.

Formatos y documentos

El proponente seleccionado deberá diligenciar todos los formatos y documentos establecidos por el Ministerio TIC, que conforman el modelo integrado de gestión - MIG -, entre ellos, acuerdos de confidencialidad firmados por el representante legal, como todo equipo técnico destinado a la ejecución del contrato.

CUMPLIMIENTO LEY 1581 DEL 2012

En línea con la disposición de la política de protección de datos personales del Ministerio TIC actualizada mediante Resolución 0448 de 2022, el contratista debe garantizar el cumplimiento de los dispuesto en dicha resolución, de conformidad con lo señalado en el parágrafo del Artículo 6: Identificación del responsable y/o encargado del tratamiento.

El MinTIC, dispone: Que los titulares de los datos personales cuyo tratamiento realiza el Ministerio, tienen los siguientes derechos:

- Acceder los datos personales que hayan sido objeto de Tratamiento conforme a lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Conocer, actualizar y rectificar los datos personales frente al responsable del Tratamiento y al Encargado del Tratamiento. El derecho de actualizar y rectificar los datos se podrá ejercer, entre otros datos, en relación con datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos datos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada al responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, con respecto del uso que les ha dado a los datos personales. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a la Constitución, a la Ley 1581 de 2012 y a las demás normas que la reglamenten modifiquen o subroguen.