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)*

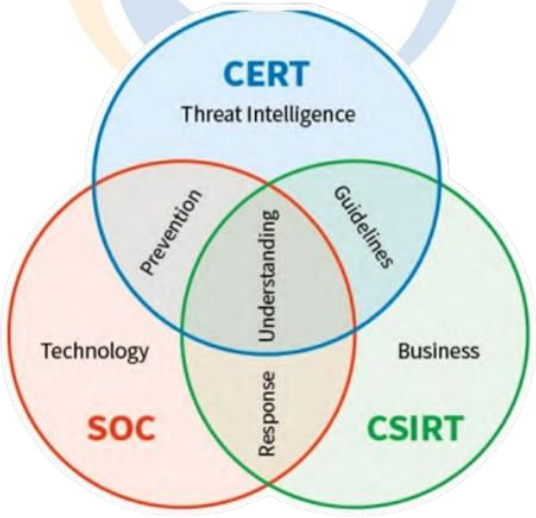

Figura 1: Relación CERT/CSIRT/SOC
Fuente: Exabeam

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 el CERT Nacional, el CSIRT de Gobierno 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 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 de 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 el gobierno de Colombia 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 del gobierno, 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 5:** Monitorización de Información Crítica
- **Componente 6:** Plataforma de entrenamiento para equipos Red y Blue
- **Componente 7:** Transferencia de Conocimiento

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

IMPLEMENTACIÓN DEL COMPONENTE DE MONITORIZACIÓN DE INFORMACIÓN CRÍTICA

MONITORIZACIÓN DE INFORMACIÓN CRÍTICA	
ÍTEM	**DESCRIPCIÓN**
1.	El componente nube provisto por la empresa proponente debe permitir controlar y gestionar quién y cuándo accede a la documentación de la entidad designada por la Corporación Colombia Digital, incluyendo la capacidad de monitorear estos accesos (quién accede, accesos bloqueados, etc.), independientemente de si la documentación está dentro de la organización o en redes o equipos externos.
2.	El componente nube provisto por la empresa proponente debe controlar el uso de la documentación, incluyendo ver, editar, imprimir, copiar y pegar.
3.	El componente nube provisto por la empresa proponente debe estar contar con la capacidad para un total de 100 usuarios de protección, permitiendo que estos usuarios puedan proteger documentación y acceder a la documentación protegida según los permisos asignados.
4.	El componente nube provisto por la empresa proponente debe permitir, proteger la información confidencial de las infraestructuras críticas del país.
5.	El componente nube provisto por la empresa proponente debe proteger la documentación gestionada por la entidad designada por la Corporación Colombia Digital, asegurando que esté libre de accesos indebidos y bajo control en todo momento, incluso si se encuentra en equipos externos o infraestructuras fuera del control directo de la entidad designada por la Corporación Colombia Digital.
6.	El componente nube provisto por la empresa proponente debe permitir la protección de documentos mediante cifrado para usuarios individuales (internos o externos), grupos de usuarios de Directorio Activo, e incluso dominios completos.
7.	El componente nube provisto por la empresa proponente debe ser una solución en modo Cloud/SaaS, sin necesidad de implantar o mantener infraestructura de servidor.
8.	La infraestructura Cloud debe integrarse con el Directorio Activo de la entidad designada por la Corporación Colombia Digital, permitiendo a los usuarios trabajar con sus credenciales de dominio y usar grupos internos del Directorio Activo para proteger la información.
9.	El componente nube provisto debe proporcionar una infraestructura Cloud/SaaS con alta disponibilidad y balanceo de carga para garantizar los mejores estándares de disponibilidad del servicio.
10.	El componente nube provisto por la empresa proponente debe permitir aplicar permisos y restricciones sobre la documentación según el tipo de confidencialidad. Los usuarios podrán aplicar permisos como ver, editar, imprimir, copiar, pegar, y controlar el acceso de terceros.
11.	El componente nube provisto por la empresa proponente debe poder integrarse con AD/LDAP y soportar diferentes directorios activos con o sin relación de confianza. La solución debe permitir el aprovisionamiento o anulación de usuarios desde la plataforma a través de AD.
12.	El componente nube provisto por la empresa proponente debe proporcionar al administrador acceso a auditorías de todos los documentos protegidos, incluyendo accesos y desprotecciones, así como estadísticas de uso, como documentos más accedidos y usuarios más activos.
13.	El componente nube provisto por la empresa proponente debe ser compatible con cualquier versión de Office desde Office 2003, y permitir a los usuarios acceder y trabajar con documentos protegidos en Windows, Mac OSX, iOS, Android y Linux sin necesidad de instalar software adicional.
14.	El componente nube provisto por la empresa proponente debe permitir la compartición y protección de ficheros ofimáticos y PDFs, asegurando el acceso y edición desde cualquier plataforma y navegador, sin necesidad de agentes adicionales.

15.	El componente nube provisto por la empresa proponente debe incluir capacidades para la revocación de documentos, establecimiento de marcas de agua dinámicas, y control de acceso a documentos protegidos por IP/Subnet.
16.	El componente nube provisto por la empresa proponente debe permitir la apertura de documentos de forma offline sin requerir conexión previa a Internet, garantizando el acceso a la información protegida sin restricciones innecesarias.
17.	El componente nube provisto por la empresa proponente debe permitir la integración con sistemas de gestión de documentos a través de CMIS, soluciones DLP, y herramientas de clasificación, asegurando la protección automática de la información clasificada y su seguimiento.
18.	El componente nube provisto por la empresa proponente debe permitir la protección de cuerpos de mensajes y archivos adjuntos desde Outlook, con capacidades para limitar permisos de acceso y establecer fechas de expiración para la información enviada.
19.	El componente nube provisto por la empresa proponente debe tener la capacidad de proteger automáticamente los documentos que sean movidos o copiados a determinadas carpetas de un servidor de ficheros. Esta funcionalidad debe ser transparente para los usuarios finales, garantizando que todos los documentos almacenados en servidores de ficheros Windows, NAS, etc., queden protegidos automáticamente.
20.	El componente nube provisto por la empresa proponente debe permitir a los usuarios proteger carpetas dentro de sus dispositivos, de manera que cuando un documento se copie o mueva a la carpeta, se proteja automáticamente sin intervención adicional.
21.	El componente nube provisto por la empresa proponente debe tener la capacidad de aplicar protecciones automáticas a librerías de SharePoint (2010 y versiones más recientes, on-premise, online, Office 365), de forma que cuando los usuarios suban documentos, estos queden protegidos automáticamente. Asimismo, debe proteger automáticamente la documentación subida a OneDrive sin intervención del usuario.
22.	El componente nube provisto por la empresa proponente debe proteger automáticamente el contenido subido a soluciones de almacenamiento en la nube como Box, Dropbox, y Google Drive, añadiendo una capa de protección a los documentos, incluso después de ser descargados, y limitando los derechos de uso sobre los mismos.
23.	El componente nube provisto por la empresa proponente debe integrarse con sistemas de gestión de documentos compatibles con CMIS (Content Management Interoperability Services), asegurando que los documentos almacenados en el gestor documental estén protegidos automáticamente, con permisos que viajan con el documento independientemente de su ubicación.
24.	El componente nube provisto por la empresa proponente debe soportar una amplia gama de plataformas y formatos de documento, incluyendo Windows XP SP3 hasta Windows 10, Office 2003 hasta Office 2019 y Office 365, y formatos como PDF, MS-Word, MS-Excel, MS-PowerPoint, XPS, imágenes (jpg, png, bmp, etc.), video (.mp4, .avi, .wmv), y audio (.mp3).
25.	El componente nube provisto por la empresa proponente debe ser capaz de proteger documentos CAD de herramientas como AutoDesk AutoCAD, Siemens SolidEdge, Dassault Systemes CATIA y SolidWorks, asegurando que los formatos de archivo específicos (como .dwg, .ipt, .asm) se puedan proteger y gestionar según las políticas de la organización.
26.	El componente nube provisto por la empresa proponente debe ser compatible con suites de lectura y edición de documentos como Adobe Reader, Adobe Acrobat, Foxit Reader, Foxit Phantom, Nuance PDF, Nitro PDF, y Microsoft Office, permitiendo la protección y acceso sin necesidad de instalar software adicional en el dispositivo del usuario.
27.	El componente nube provisto por la empresa proponente debe permitir la protección de correos electrónicos directamente desde Outlook, incluyendo la capacidad de proteger tanto

	el cuerpo del mensaje como los archivos adjuntos, establecer permisos de acceso, fechas de expiración y la posibilidad de revocar el acceso de forma remota.
28.	El componente nube provisto por la empresa proponente debe ser capaz de proteger documentos automáticamente en tránsito, como aquellos copiados o movidos desde USBs o unidades de red, asegurando que la información confidencial esté protegida en todo momento.
29.	El componente nube provisto por la empresa proponente debe permitir a los usuarios realizar un seguimiento de los documentos protegidos, incluyendo quién ha accedido, cuándo, y qué acciones se han realizado. También debe permitir revocar accesos y modificar permisos en tiempo real, independientemente de la ubicación del documento.
30.	El componente nube provisto por la empresa proponente debe integrarse con soluciones DLP (Data Loss Prevention), permitiendo la protección automática de documentos clasificados como confidenciales y seguimiento del acceso a estos documentos. Debe ser compatible con DLPs de Symantec, ForcePoint, Trellix, y Microsoft.
31.	El componente nube provisto por la empresa proponente debe permitir la protección automática de información clasificada según etiquetas o herramientas de clasificación. Debe ser compatible con las principales herramientas de clasificación del mercado, como Boldon James, Titus, Janus y Tukan, y aplicar políticas de protección basadas en la clasificación asignada.
32.	El componente nube provisto por la empresa proponente debe soportar el acceso y la protección de documentos en múltiples plataformas móviles y sistemas operativos, incluyendo Android, iPhone, iPad, y Mac OSX, asegurando la disponibilidad de funcionalidades de protección en estos entornos.

IMPLEMENTACIÓN DEL COMPONENTE DE ENTRENAMIENTO PARA EQUIPOS RED Y BLUE

ENTRENAMIENTO PARA EQUIPOS RED Y BLUE	
ÍTEM	**DESCRIPCIÓN**
1.	El componente nube provisto por la empresa proponente debe ser contar con una plataforma en infraestructura SaaS avanzada diseñada para el entrenamiento continuo y exhaustivo de los equipos de respuesta a incidentes, específicamente para los equipos blue y red teams. Debe facilitar simulaciones realistas de ataques cibernéticos, permitiendo la práctica de habilidades en un entorno controlado y seguro. La empresa proponente asumirá los componentes necesarios para el funcionamiento en la nube.
2.	El componente nube provisto por la empresa proponente debe tener la capacidad de realizar simulaciones persistentes que reflejen escenarios de ataques reales, mejorando así la preparación y respuesta del equipo frente a amenazas auténticas.
3.	El componente nube provisto por la empresa proponente debe incluir un módulo de gestión de crisis especializado para la simulación de situaciones de crisis a nivel estratégico, que permita evaluar la toma de decisiones críticas durante incidentes de gran impacto y trascendencia nacional.
4.	El componente nube provisto por la empresa proponente debe ser capaz de integrar y utilizar información de incidentes previos y datos actuales de seguridad, identificados por las herramientas y soluciones en uso por el la entidad designada por la Corporación Colombia Digital, para asegurar que las simulaciones sean lo más realistas y útiles posible.

5.	El componente nube provisto por la empresa proponente debe permitir la descarga de todas las muestras de la librería sin límite para los usuarios, con las muestras comprimidas con contraseña para mayor seguridad.
6.	El componente nube provisto por la empresa proponente debe permitir la carga de muestras externas a la plataforma (Bring Your Own Malware - BYOM), para personalizar aún más la librería de muestras.
7.	El componente provisto por la empresa proponente debe contar con paquetes de muestras reales de amenazas conocidas, modificadas y avanzadas.
8.	El componente provisto por la empresa proponente debe tener la capacidad de realizar un número ilimitado de ejecuciones, donde cada paquete enviado en la emulación represente comportamientos de diferentes ciberactores, permitiendo pruebas efectivas que cubren las diferentes etapas y fases de un ataque.
9.	El componente provisto por la empresa proponente debe crear y poner a disposición de sus usuarios artefactos con capacidades de callback reales, como interruptores de emergencia (killswitch) o descargas de malware.
10.	El componente provisto por la empresa proponente debe tener la capacidad de forzar la evasión de elementos de ciberseguridad basados en sandboxing y hashes a través de un algoritmo de envío y control basado en encriptación asimétrica, verificando el correcto funcionamiento de soluciones de seguridad avanzadas que validan cada artefacto que viaja por la red, incluso con mecanismos avanzados de ofuscación y encriptación.
11.	El componente provisto por la empresa proponente debe tener la capacidad de usar muestras reales para las emulaciones de ataques, con un mínimo de las siguientes categorías: • Malware regular • Artefactos personalizados • Artefactos Forced Zero Day
12.	El componente provisto por la empresa proponente debe soportar un máximo de 30 escenarios y 50 usuarios concurrentes.
13.	El componente provisto por la empresa proponente debe permitir la simulación en dispositivos de cualquier tecnología utilizada en las infraestructuras tecnológicas estándar.
14.	El componente provisto por la empresa proponente debe estar disponible para ser activada y utilizada a demanda por el equipo de la entidad designada por la Corporación Colombia Digital, según las necesidades de entrenamiento y las simulaciones programadas para cada una de las entidades públicas y privadas.
15.	El componente provisto por la empresa proponente debe contar con una interfaz de usuario amigable que facilite la programación, monitorización y análisis de las simulaciones sin necesidad de extensos conocimientos técnicos.
16.	El componente provisto por la empresa proponente debe generar informes detallados post-simulación que proporcionen análisis de rendimiento y recomendaciones para mejoras futuras en las estrategias de seguridad.
17.	El componente provisto por la empresa proponente debe recibir actualizaciones continuas para asegurar que las simulaciones reflejen las últimas tácticas, técnicas y procedimientos usados por los adversarios.
18.	El componente provisto por la empresa proponente debe proporcionar un soporte técnico robusto para resolver cualquier problema operativo o técnico que pueda surgir.

IMPLEMENTACIÓN Y ADECUACIÓN FÍSICA DEL SOC NACIONAL

La consolidación de un SOC Nacional requiere la integración de componentes tecnológicos de última generación, capaces de soportar la carga operativa y las demandas de un entorno de ciberseguridad avanzado. Esto exige una infraestructura robusta que permita la integración de todos los sistemas, redes, y tecnologías de monitoreo, lo cual implica adecuaciones en el espacio físico para optimizar la operatividad y facilitar el trabajo de los analistas. Además, estas adecuaciones deben incluir todos los elementos tecnológicos necesarios para el óptimo funcionamiento y expansión del SOC Nacional.

Con el fin de asegurar la eficiencia del SOC Nacional, es crucial realizar el mantenimiento o reemplazo de ser necesarios de los elementos que componen la solución de videowall actual compuesta por un arreglo de 6x3 de 55" que permita a los equipos de seguridad visualizar y analizar en tiempo real los flujos de datos críticos. Este elemento requiere de un entorno adecuadamente acondicionado que garantice visibilidad, accesibilidad y una operación continua sin interrupciones. Además de la instalación del videowall, resulta fundamental la integración de otros componentes avanzados, como (2) servidores que permitan el crecimiento futuro del SOC y la respuesta a potenciales incidentes de ciberseguridad.

Asimismo, para el desarrollo exitoso del SOC Nacional, se debe tener en cuenta la estética y funcionalidad del espacio. Esto implica el embellecimiento del entorno laboral, asegurando un espacio ergonómico y cómodo para los operadores, a fin de que puedan trabajar de manera eficiente y segura.

UBICACIÓN DEL SOC NACIONAL

El SOC Nacional se deberá instalar en todos sus componentes y adecuaciones en las instalaciones de la entidad designada por la Corporación Colombia Digital, ubicado en la ciudad de Bogotá D.C.

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.

TRANSFERENCIA DE CONOCIMIENTO

La empresa proponente seleccionado debe desarrollar y ejecutar un programa de transferencia de conocimiento para un mínimo de diez (10) de los analistas de seguridad de la entidad designada por la Corporación Colombia Digital. Este programa garantizará que el equipo esté plenamente capacitado para operar y maximizar las funcionalidades de cada una de las herramientas y soluciones tecnológicas implementadas.

METODOLOGÍA DE CAPACITACIÓN:

Cada servicio requerirá mínimo de 20 horas de capacitación, distribuidas de manera efectiva para cubrir todos los aspectos necesarios de instalación, implementación y operación. Se deben realizar mínimo diez (10) sesiones presenciales de mínimo cuatro (4) horas en las instalaciones de la entidad designada por la Corporación Colombia Digital, estas sesiones cubrirán aspectos funcionales, de configuración y operativos de todos los componentes contratados en el presente proyecto.

La transferencia de conocimiento debe ser impartida por el equipo implementador de la empresa proponente, esta se debe llevar a cabo durante el periodo de implementación y post-implementación; se debe proporcionar manuales digitales, guías de usuario digitales y recursos en línea provistos directamente del fabricante para complementar la formación presencial.

Estas capacitaciones, deben ser ejecutadas en el sitio que convengan el supervisor del contrato y el contratista, una vez suscrita el acta de inicio del contrato.

CURSOS Y VOUCHER

La empresa proponente debe suministrar curso + Voucher de certificación para el equipo de la entidad designada por la Corporación Colombia Digital en las siguientes certificaciones:

- Auditor Líder ISO 27001 última versión para mínimo cinco (5) Personas
- Certified Threat Intelligence Analyst (CTI-A) para mínimo tres (3) personas
- Certificación Red vs Blue para mínimo dos (2) personas.

La disponibilidad se medirá usando la siguiente ecuación: $\left(1 - \frac{Número\ total\ de\ minutos\ que\ la\ herramienta\ no\ está\ disponible}{Número\ de\ días\ en\ el\ mes\ x24\ horas\ x60\ minutos}\right) x100\%$ La indisponibilidad es el número total de minutos, durante el mes, en los que la herramienta no está disponible, dividido en el número total de minutos en el mes. La medición se hace de manera independiente para cada una de las herramientas, para lo cual el proveedor realizara el monitoreando permanentemente a cada uno de ellos durante el mes. Los resultados del monitoreo son mantenidos por el proveedor para que puedan ser consultados por Equipo 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 de la entidad designada por la Corporación Colombia Digital, teniendo en cuenta lo definido en los numerales del presente capítulo.

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

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

confidencialidad, para garantizar la reserva de la información del 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 la entidad designada por la Corporación Colombia Digital, 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 la entidad designada por la Corporación Colombia Digital, 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 de la entidad designada por la Corporación Colombia Digital, 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 de la entidad designada por la Corporación Colombia Digital 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 la entidad designada por la Corporación Colombia Digital, 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 la entidad designada por la Corporación Colombia Digital, 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 de la entidad designada por la Corporación Colombia Digital 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.

La entidad designada por la Corporación Colombia Digital, dispone: Que los titulares de los datos personales cuyo tratamiento realiza la entidad designada por la Corporación Colombia Digital, 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.